HiSpeed Fast Ethernet Switch

Troubleshooting Guide

HITACHI
internetworking

Part No. US7070447-001, Rev 01

Trademarks

HiSpeed and HiView are trademarks of Hitachi Computer Products (America), Inc.

All other brand and product names are trademarks of their respective holders.

Copyrights

© 1997 Hitachi Computer Products (America), Inc.
All Rights Reserved.

Technical Support

The Hitachi internetworking Solution Center provides technical assistance and information free of charge during the initial warranty period on hardware and software products. When you call, please have the following information on hand:

- Your name, address, telephone, and fax number
- Type of equipment, serial number, and software version number
- A description of any commands entered and the resulting output
- Whether you were trying to connect to other equipment

Hitachi internetworking Solution Center:

Hours:	Monday – Friday, 7a.m. to 6p.m. Pacific time
Phone:	408-588-3119 or 1-800-611-4551
Fax:	408-988-9156
E-mail:	hi-assist@hitachi.com
WWW Browser:	http://www.internetworking.hitachi.com/solution.center

If you purchased your product(s) from an Hitachi reseller, you should contact your reseller for technical support.

First Edition (August, 1997). The information in this manual applies to the Hitachi HiSpeed switch, software version 1.3 or later.

Hitachi Computer Products (America), Inc. is not liable for any errors or omissions in this manual, nor for any injury or damage that results from the use of it.

No part of this manual may be reproduced in any form by any means — graphic, electronic, or mechanical, including, but not limited to photocopying, recording, transmitting, transcribing, scanning, or storage in any retrieval system or translated into any language without the prior written permission of:

Hitachi Computer Products (America), Inc.
3101 Tasman Drive
Santa Clara, California 95054

Table of Contents

Chapter 1
Introduction

Purpose of the Guide 1-1
Basic Troubleshooting Tips 1-1
How to Contact Tech Support 1-2

Chapter 2
HiSpeed Switch

What is the HiSpeed Switch? 2-1
Basic Product Features Supported 2-1
Available Configurations 2-2
HS140/150-010 Model 2-4
HS140/150-100 Model 2-4
Expansion Modules 2-5
UpLink Modules 2-6

Chapter 3
Hardware Diagnostics

Observing LEDs 3-1
Reset Button 3-2
LEDs 3-2
Reset Button 3-3
HiSpeed Memory, Boot Prom, Flash Components 3-5
Factory Switch Settings 3-5

Chapter 4
Cabling

Basic Connections 4-1
10BASE-TX Ports 4-2
10/100BASE-TX Ports 4-3
100BASE-FX Ports 4-3
Console Port 4-4

Chapter 5
Fundamentals of Networking

Layer 1: Physical Layer 5-2
Layer 2: Data Link Layer 5-2
Layer 3: Network Layer 5-3
Layer 4: Transport Layer 5-3
Layer 5: Session Layer 5-3
Layer 6: Presentation Layer 5-3
Layer 7: Applications Layer 5-3

Chapter 6
Methods of Managing the Switch

CLI (Command Line Interface) 6-1
Using the Console Port 6-1
Troubleshooting a Console Connection 6-2
Using a Telnet Session 6-2
Troubleshooting a Telnet Session 6-3
Logging In 6-3
Troubleshooting the Login Procedure 6-3

HiView Switch Management 6-4
Windows 95/Windows NT 4.0 6-4
UNIX 6-5
HiView Tips 6-5
Windows 95/NT 4.0 6-5
HiView Tips 6-5
UNIX 6-5
Troubleshooting HiView 6-6
Troubleshooting Network Management software on the HiSpeed switch 6-6
SNMPC Issues 6-6
EXAMPLE: 6-7
MeterWare Issues 6-7
SNMPTalk Issues 6-10

Chapter 7
Bridging Concepts

Basic Bridging Concepts 7-1
How Spanning Tree Works 7-1
Troubleshooting Bridging Issues 7-3
CLI Commands 7-5

Chapter 8
VLAN Concepts

Troubleshooting VLANs 8-3
VLAN Tips 8-4

Chapter 9
Troubleshooting at the MAC Layer

Ethernet 9-1
Physical Media Specifications 9-2
Common Ethernet Errors 9-2
Ethernet Tips 9-3
Troubleshooting Ethernet 9-4
CLI Commands 9-5

Chapter 10
Troubleshooting at the Network Layer

IP (Internet Protocol) 10-1
Other IP-related Services 10-2
RIP (Routing Information Protocol) 10-2
Route Cache Forwarding vs. IP Forwarding 10-3
Static Routes vs. Dynamic Routes 10-3
Default Route 10-3
Common ICMP Destination Unreachable Messages 10-4
Network Unreachable 10-4
Host Unreachable 10-4
Port Unreachable 10-4
Troubleshooting IP 10-5
CLI Commands 10-6

Chapter 11
Basic ATM Concepts

Permanent Virtual Circuits vs.
Switched Virtual Circuits 11-2
LAN Emulation (LANE) 11-2
LAN Emulation Client (LEC) 11-3
LAN Emulation Configuration Server 11-3
LAN Emulation Server (LES) 11-3
Broadcast and Unknown Server (BUS) 11-3
Classical IP over ATM (CIP) 11-4
Point-to-Point Bridging (PTOP) 11-4
Trunking 11-5
Hitachi HiSpeed ATM Specifications 11-6
ATM Troubleshooting Tips 11-6
Troubleshooting LANE 11-7
Troubleshooting CIP 11-8
Troubleshooting PTOP 11-10
Troubleshooting Trunking 11-12
CLI Commands 11-14

Chapter 12
FDDI Concepts

HiSpeed FDDI Uplink 12-2
Cable Connections 12-3
Observing LEDs 12-4
FDDI Bridge Modes 12-4
Filtering Mode 12-5
Forwarding Mode 12-5
Promiscuous Mode 12-5
FDDI Troubleshooting Tips 12-5
Troubleshooting FDDI: 12-6
CLI Commands 12-9

Index

List of Figures

Figure 2-1. Model HS140-010 base model with an HS-150-010-16E expansion module installed 2-4
Figure 2-2. HS150-100-16 base model with an HS150-100-8E expansion module installed 2-5
Figure 3-1. Module LEDs 3-2
Figure 5-1. Network Media 5-2
Figure 6-1. MIB Compiler 6-8
Figure 6-2. Fig2. MIB Browser 6-9
Figure 7-1. Using Spanning Tree 7-2
Figure 8-1. VLANs 8-2
Figure 11-1. VPI/VCI 11-1
Figure 11-2. ATM LANE 11-2
Figure 11-3. ATM CIP 11-4
Figure 11-4. ATM PTOP 11-5
Figure 11-5. ATM Trunk 11-5
Figure 12-1. HS150 on an FDDI network 12-1
Figure 12-2. FDDI Uplink Module installed in an HS150 12-2
Figure 12-3. SAS cable connections 12-3
Figure 12-4. DAS cable connections 12-3

List of Tables

Table 2-1.	Base model configurations	2-3
Table 2-2.	HiSpeed switch expansion modules	2-5
Table 2-3.	Uplink modules for the HS15-010 and HS150-100	2-6
Table 3-1.	LED status	3-2
Table 3-2.	RJ-45 LEDs	3-4
Table 3-3.	LEDs on FX ports	3-4
Table 4-1.	RJ-45 Connector pin assignments	4-2
Table 4-2.	Console Port Pin Assignments	4-4
Table 8-1.	VLAN Entries	8-4
Table 8-2.	Useful CLI Commands	8-4
Table 10-1.	IP address classes	10-1
Table 12-1.	LED States	12-4

Chapter 1
Introduction

Purpose of the Guide

The purpose of this troubleshooting guide is to assist users in understanding, identifying and diagnosing network related problems in a switched network environment. Additionally, the guide allows users to gain a better understanding of the Hitachi's HiSpeed switch functionality, features, and performance.

Note: This guide is not intended to replace any of the HiSpeed User and Installation Guides. It is designed as a troubleshooting tool only and serves to compliment existing HiSpeed documentation.

Basic Troubleshooting Tips

To isolate a network-related problem, one approach is to first eliminate all known possibilities. This methodology is referred to as 'divide and conquer.' By using this technique, the problemis divided into smaller components, making it easier to isolate and identify the problem. To avoid overlooking the obvious when focusing on a specific problem, ask yourself the following questions:

- ❒ Has this functionality ever worked before? When did this problem start happening?
- ❒ What recent changes have been made to the network? Software upgrade? Devices added to the network?
- ❒ Are you running the latest version of software?
- ❒ Do you have the latest version of Release Notes?

- ❒ Are all users affected? Or a certain group of users on a specific segment?
- ❒ Are all types of traffic affected? In other words, what protocols are failing?
- ❒ Is the problem consistent or intermittent?
- ❒ Can the users ping themselves? If so, can they ping the gateway and beyond?
- ❒ Have you tried resetting the switch?

How to Contact Tech Support

For technical support, contact Hitachi's Internetworking Solution Center:

Hours:	Monday - Friday, 7 a.m. to 6 p.m. Pacific Standard Time (PST)
Phone:	1-800-611-4551 or 408 -588-3119
Fax:	408 -988 -9156
E-mail:	hi-assist@hitachi.com
WWW:	http://www.internetworking.hitachi.com/solution.center

To expedite the troubleshooting process, please have the following information available when contacting Hitachi Technical Support.

- ❒ Model and serial number of the switch
- ❒ Version of firmware, boot prom
- ❒ File size of firmware
- ❒ Operational status of the following LEDs:
  - System
  - Power
  - Link
  - Diagnostics & Activity
- ❒ Error messages being reported to the console
- ❒ network diagram
- ❒ Sniffer trace on the affected segment (if required)
- ❒ dispcfg.dat

Abatch program called ***dispcfg*** is available on Hitachi's anonymous FTP server (204.48.18.63). When used in combination with HiSpeed's debugging commands, relevant configuration on the switch is captured and the results are written to the file ***dispcfg.dat***. Refer to ***dispcfg.doc*** for instructions on how to run the batch program. Forward the results to Hitachi's Technical Support Team via the WEB or email.

If using a browser, type in the following URLs to download the files:

```
ftp://ftp.hicam.hitachi.com/outgoing/dispcfg
ftp://ftp.hicam.hitachi.com/dispcfg.doc
```

Please email any suggestions/comments on the Troubleshooting Guide to:

HIassist@hitachi.com

Chapter 2
HiSpeed Switch

What is the HiSpeed Switch?

The HiSpeed switch is a multiprotocol, Fast Ethernet workgroup switch than can be configured for up to 32 10/100 Mbps LAN switch ports, depending on the model. The HiSpeed switch maximizes performance in existing shared media LANs by allowing up to 32 separate collision domains on a per port basis. By segmenting the network in this fashion, the amount of collisions are reduced and the available network bandwidth is optimized.

The HiSpeed switch offers the scalability and flexibility to accept a range of high speed interfaces for connecting to FDDI, ATM and WAN backbones.

Basic Product Features Supported

The HiSpeed switch includes the following hardware and software product features:

- ❒ Virtual LAN (VLAN) support for 10BASE-T Ethernet and 100BASE-T Fast Ethernet VLANs, including VLANs over ATM virtual connections
- ❒ Loop detection using Spanning Tree Protocol (IEEE 802.1d)
- ❒ Virtual Routing to provide switching between VLANs
- ❒ Front panel LEDs that provide operating status
- ❒ Reset button for front panel control of switch
- ❒ RS-232C console port interface for local access to the switch
- ❒ Rack mount or table mount capabilities

- Supports multiple hardware configurations and provides support for the following port configurations:
  - 10BASE-TX ports
  - 10/100BASE-TX ports
  - 100BASE-FX ports
  - PCI-based ATM Uplink to server
  - PCI-based FDDI Uplink to server
- Supports field-upgradeable expansion modules for maximum customization
- Supports Autonegotiation on all 10/100 Mbps ports
- Supports full- or half-duplex on all 10/100BASE-TX ports
- Provides port mirroring to allow monitoring of the activities of one port from another port
- Provides flow control to autosense buffer limits on the transmit port
- Supports Group 1, 2, 3, and 9 RMON
- Supports Simple Network Management Protocol (SNMP) agent for Management Information Bases (MIB) II and a private enterprise MIB
- Provides a service port for console connection to locally or remotely configure and manage the switch

Available Configurations

The HiSpeed switch is available from the factory fully or partially populated. The expansion slot on the switch provides for field customization to meet the changing needs of the network.

The HiSpeed switch is available in two base model configurations:

- HS140/150-010
- HS140/150-100

Each of the HS150 and HS140 models has one expansion slot which can be populated with an expansion module that doubles the number and/or type of available ports. The expansion modules can be installed in the field or at the factory prior to shipment. The HS150 switch models also have a PCI bus for the addition of an uplink module. The uplink module provides a dedicated connection to a server or network backbone. Table 2-1 lists the model numbers and the upgrade path for each.

Note: The HS140-010 and HS140-100 models are not capable of accepting the uplink options.

Table 2-1. Base model configurations

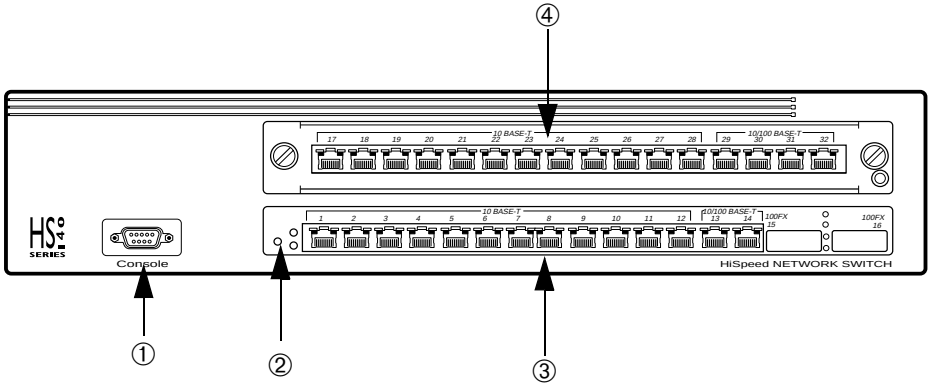
Model	10 Mbps TX Ports	10/100 Mbps TX Ports	100 Mbps FX Ports	Total Ports	Uplink	Upgrades To
HS 150-010-16	12	4	0	16	Yes	To 32 ports with HS150-010-16-E
HS 150-010-32	24	8	0	32	Yes	Max port configuration
HS140-010-16-2FX	12	2	2	16	No	Max configuration.
HS140-010-32-2FX	24	6	2	32	No	Max port configuration
HS 150-100-8	0	8	0	8	Yes	To 16 ports with HS150-100-8-E or HS150-100-8-FXE
HS 150-100-16	0	16	0	16	Yes	Max port configuration
HS 140-100-16	0	16	0	16	No	Max port configuration
HS 140-100-8-FX	0		8	8	No	To 16 ports with HS150-100-8-E or HS150-100-8-FXE
HS 140-100-16-FX	0		16	16	No	Max port configuration
HS140-100-16-8FX	0	8	8	16	No	Max port configuration

Note: HS140-010 switch units accept HS150-010 expansion modules and HS140-100 switch units accept HS150-100 expansion modules.

HS140/150-010 Model

The -010 models ship with a sixteen port module configured in the captive slot. This module can consist of 10BASE-TX, 10/100BASE-TX or 100BASE-FX type ports and can be configured with either all one type of port or a combination of three types of ports. The expansion slot is capable of accepting an additional 16 ports for a total of 32 ports per switch.

Figure 2-1 shows an HS140-010 switch model with the expansion slot populated by an HS-150-010-16E (12 10BASE-T ports and four 10/100BASE-TX ports) expansion module and no uplink capability.



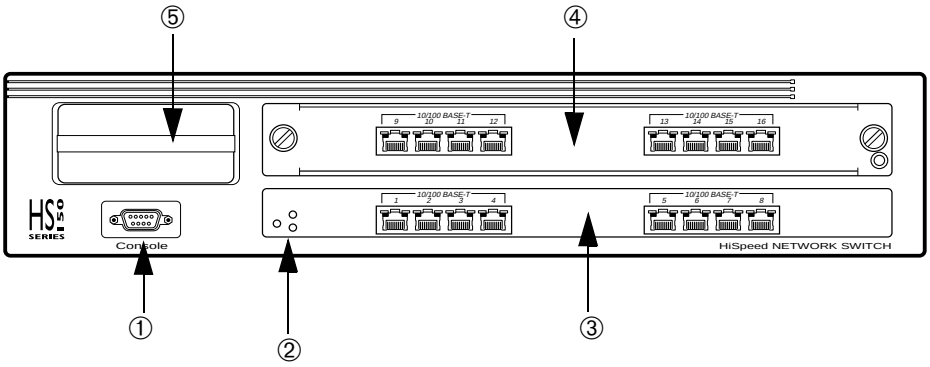
Key: ① Console port
② Reset button/Power LED
③ Onboard module
④ Expansion module

Figure 2-1. Model HS140-010 base model with an HS-150-010-16Eexpansion module installed

HS140/150-100 Model

The -100 models ship with an eight port module configured in the captive slot. This module can consist of either eight ports of 10/100BASE-TX or eight ports of 100BASE-FX type ports. The expansion slot is capable of accepting an additional 8 ports for a total of 16 ports per switch.

Figure 2-2 shows an HS150-100 model with an 8-port TX expansion module (no uplink module installed).



Key: ① Console port
② Reset button/Power LED
③ Onboard module (with TX ports)
④ Expansion slot (with TX ports)
⑤ UpLink slot

Figure 2-2. HS150-100-16 base model with an HS150-100-8E expansion module installed

Expansion Modules

There are currently three expansion modules available to upgrade or reconfigure the capacity of the base models. Table 2-2 lists the available expansion modules.

Table 2-2. HiSpeed switch expansion modules

Module Number	10 Mbps TX Ports	10/100 Mbps TX Ports	100 Mbps FX Ports	Base Model
HS150-010-16-E	12	4	0	HS140/150-010
HS150-100-8-E	0	8	0	HS140/150-100
HS150-100-8-FXE	0	0	8	HS140/150-100

UpLink Modules

The uplink module is installed into the uplink slot located in the upper left corner of the front panel. The uplink provides high-speed server access for FDDI and ATM. Only the HS150-010 and -100 models accommodates the uplink. Table 2-3 lists the available uplink modules.

Table 2-3. Uplink modules for the HS15-010 and HS150-100

Model	Ports	Type	Base Model
HS150-ATM-UL	1	Fiber Optic	ATM LANE uplink module
HS150-FDDI-UL	DAS/SAS	Fiber Optic	FDDI uplink module
HS150-FR-UL	1	X.25	Frame Relay/X.25 uplink module

Chapter 3
Hardware Diagnostics

The power and status LEDs indicate the general operations of the HiSpeed switch. The HiSpeed switch provides transparent operation once it has been installed and configured. If you suspect that it may be malfunctioning or causing a system problem, check the status of the LEDs. Call Technical Support to report the condition.

In addition to the built-in LEDs on the switch, there is an Integrated System Diagnostic (ISD) software which tests the system to determine any hardware failures. The system diagnostic's focus is to help identify and verify major system features and components such as the processor, memory, I/O devices, system buses, packet switch and uplink interfaces on the switch.

The ISD software (**`isd`**) and download instructions (**`isd.doc`**) are available on the Hitachi anonymous FTP server, 204.48.18.63. If you are using a browser, type in the following URLs to download the files:

```
ftp://ftp.hicam.hitachi.com/outgoing/isd
ftp://ftp.hicam.hitachi.com/outgoing/isd
```

Observing LEDs

LEDs are located on each module and on the RJ-45 port connectors. Figure 3-1 shows the LED configurations,

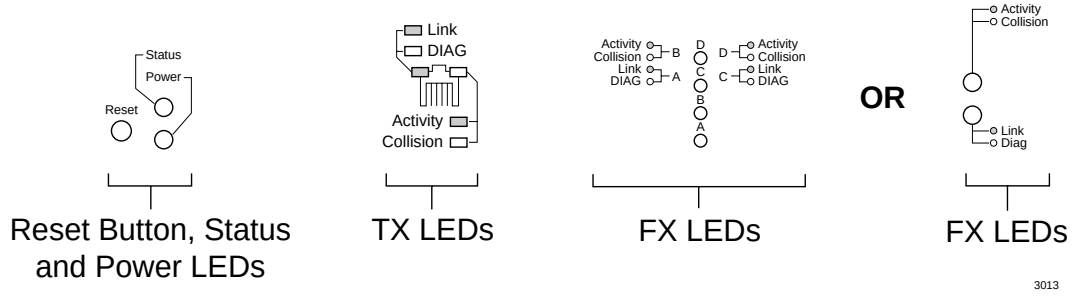


Figure 3-1. Module LEDs

Reset Button

The Reset button, located on the front panel of the switch, allows you to manually recycle power and reset the switch. Pressing the Reset button initiates a warm boot of the system and generates power-on self test (POST) and diagnostics. The button is recessed into the unit to prevent accidental resets. Use the tip of a pen or pencil to reset the switch.

LEDs

Table 3-1 lists the meaning and actions of the LEDs, Table 3-2 lists the RJ-45 LED meanings, and Table 3-3 lists the meaning of the FX LEDs.

Table 3-1. LED status

LED	LED Color	Status	Action Required
System Status Indicator	Flashing green	Normal operation	None. LED should flash every second. This indicates that the switch is functioning normally.
	Solid green	Switch encountered abnormal condition	You probably cannot log in to the switch. Reboot.
	Flashing amber	Switch encountered abnormal condition	Reboot the switch.
	Solid amber	Switch encountered abnormal condition	The switch is probably still running. Try to troubleshoot the problem without rebooting the switch.
Power Indicator	Solid green	Normal operation when power is applied	None.

Table 3-1. LED status

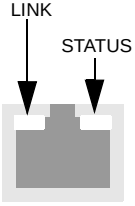
	Unlit	No power to switch	Check to see if switch is on. If so, turn it off and reboot. If LED remains unlit, replace the switch.
Port LED — Activity/Collision (green/amber)	Flashing or solid green	Normal operation when port receives or transmits traffic	None.
	Unlit	No traffic	None.
	Flashing amber	Collisions in half-duplex mode (TX only)	None.
Port LED — Link/ Diag (green)	Solid green	Good cable link status	None.
	Unlit or flashing	No link if unlit; a link problem if flashing	Try the following: verify cable, verify port speed, verify the state of the autonegotiation to ensure the port speeds match.

Reset Button

The Reset button, located on the front panel of the switch, allows you to manually recycle power and reset the switch. Pressing the Reset button initiates a warm boot of the system and generates power-on self test (POST) and diagnostics. The button is recessed into the unit to prevent accidental resets. Use the tip of a pen or pencil to reset the switch.

Each RJ-45 port has two LEDs configured into the connector. The LEDs are used to indicate link and status, as described in Table 3-2.

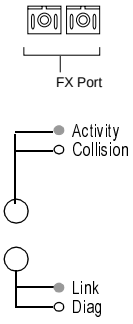
Table 3-2. RJ-45 LEDs



LED	Color	Status	Description
LINK			
Link	Green	Solid	Link is active and connected.
		Flashing	The link is interrupted
		Off	There is no link present on the port
Diag	Amber		Used by support engineers.
STATUS			
Activity	Green	Solid Flashing	LED lights when data is being received or transmitted.
		Off	There is no data transmission currently on the link.
Collision	Amber	Flashing	Collision when in half-duplex mode.

Each FX port has two LEDs to the right of the SC connector. Table 3-3 lists the LEDs and their function.

Table 3-3. LEDs on FX ports



LED	Color	State	Description
Activity	Green	Solid or Flashing	Port is receiving or sending data
		Off	No transmission on port
Collision	Amber		Currently not supported on FX ports.
Link	Green	Solid	Indicates good link with attached device
		Flashing	Indicates link to attached device is intermittent. Check cabling.
		Off	Indicates there is not link with attached device. Check cabling.
Diag	Amber		Used by support.

HiSpeed Memory, Boot Prom, Flash Components

The HiSpeed switch is shipped standard from the factory with the following system configurations.

- *Memory:*
  8 Mbytes (DRAM)
- *Boot Prom:*
  512 Kbytes (EPROM)
  - Initialization boot code
  - Power-On Self-Test (POST)
  - TFTP/FTP boot code
  - Modem remote control
  - Routines to load and execute compressed code
- *Flash:* 4 Mbytes
  - compressed system code
  - compressed systems diagnostics
  - system configuration data
  - system traces (for debugging purposes)

Factory Switch Settings

The HiSpeed switches are shipped from the factory without any IP configurations to the switch. To perform any routing and network management to the switch, you must assign an IP address to a VLAN on the switch. Otherwise, the switch will only provide core switching functionality. The factory default settings on the switch are configured as follows:

- Console speed is 9600
- Login password is switch
- All ports belong to VLAN 1
- RIP is silent
- Ethernet statistics are disabled

- ❒ Ethernet port settings: autonegotiation is ON
- ❒ Spanning Tree is enabled

These settings provide for switching in a single broadcast domain.

Chapter 4
Cabling

The HiSpeed switch models are similar in physical makeup of ports and LEDs. This section describes the following port types, LED configurations, and connections for all models.

- ❒ 10BASE-TX ports
- ❒ 10/100BASE-TX ports
- ❒ 100BASE-FX ports
- ❒ Console connection
- ❒ Reset button

Basic Connections

For communications to take place between two devices, the transmitter of one device must connect to the receiver of the other device. The connection must be achieved through a crossover function, which could be a crossover cable or a port that implements the crossover function internally. All the 10/100BASE-TX ports are wired for MDI-X (media-dependent interface-crossover). Use the proper cabling to connect to devices as follows:

- ❒ To connect to a switch, hub, or bridge, use a crossover cable.
- ❒ To connect to a workstation or file server, use a straight-thru cable.
- ❒ Autonegotiation on the 10/100BASE-TX ports is set by polling the connected device. The two devices will negotiate the speed, 10 Mbps or 100 Mbps, and select whichever is most optimal.

- Line transmission modes on the 10/100BASE-TX ports support both half-duplex and full-duplex operations. By definition, the CSMA/CD protocol is half-duplex where data can be transmitted and received in both directions, but only at one direction at a time. Therefore, 10BASE-TX ports operate in half-duplex mode only.

10BASE-TX Ports

The 10BASE-T port connections are provided for the 10 Mbps Ethernet segment or nodes to attach to the HiSpeed switch. The RJ-45 jacks accept standard Category 3, 4, or 5 copper unshielded twisted pair (UTP) cable connections. Pin assignments for the standard RJ-45 connector are given in Table 4-1. The HiSpeed switches are shipped with the 10BASE-T connectors configured as MDI-X (media-dependent interface-crossover). These ports connect over straight cables to the network interface controller (NIC) card in a node or server, similar to a conventional Ethernet repeater hub. If you are connecting to another Ethernet hub or Ethernet switch, you need a crossover cable unless an MDI connection exists on the associated port of the attaching device (see “Connecting 10BASE-T Ports” on page 2-8 for a description of the crossover cable).

The 10 Mbps ports operate in half-duplex mode only, and each port has an associated LED that indicates link status of the line.

Table 4-1. RJ-45 Connector pin assignments

Pin	MDI-X Signal
1	Receive data + (RD+)
2	Receive data - (RD-)
3	Transmit data + (TR+)
4	Not used
5	Not used
6	Transmit data - (TD-)
7	Not used
8	Not used

10/100BASE-TX Ports

The 10/100BASE-TX ports on the HiSpeed switch are standard RJ-45 connections using UTP Category 5 cabling. These ports, like the 10BASE-TX ports, are wired for MDI-X and require a crossover cable when connecting to an Ethernet hub or another switch.

Note: Since these ports are capable of operating at 100 Mbps, it is imperative that only Category 5 cabling be used.

The 10/100 Mbps ports support autonegotiation where speed is set by polling the connected device and determining which speed, 10 Mbps or 100 Mbps, is the most optimal.

The 10/100BASE-TX ports on the HiSpeed switch are designed to support both half-duplex and full-duplex operation. By definition, the CSMA/CD protocol is half-duplex. allowing either data transmission or reception, but never both at the same time. Point-to-point network connections, such as DTE-to-switch ports, allow a file server to transmit frames to a switch while simultaneously receiving frames from the same switch. This two-way, non-CSMA/CD full-duplex communication allows an effective bandwidth of 200 Mbps between two devices.

Both the port speed and the duplex mode can be set using the CLI command

```
ETHERNET/CONFIG/PORT
```

For information on these commands, refer to the *HiSpeed Switch User Guide*, document number US7070424-001, that was shipped with your switch.

100BASE-FX Ports

The 100BASE-FX ports are used to attach fiber-based 100 Mbps connections to the switch. These ports provide direct attachment to end stations, switches, or servers where multimode fiber is installed. The 100BASE-FX ports accept standard SC connections using 62.5/125 micron fiber optic cable. The 100BASE-FX ports function at full-duplex only (200 Mbps) and does not support autonegotiation.

Console Port

The console port has a DB-9 male connector used to connect a management terminal to the switch by means of a straight-through DB-9 to DB-9 standard serial port cable. Using a terminal, you can monitor the results of startup self-diagnostics, perform manual boot configuration and SNMP agent configuration, and customize your network using the supplied menus and screens.

The pin assignments for the console port are provided in Table 4-2.

Table 4-2. Console Port Pin Assignments

Pins	Signal Name
1	Not Used
2	Transmit data (TD) to terminal
3	Receive data (RD) from terminal
4	Not used
5	Common signal ground
6	Not used
7	Not used
8	Not used
9	Not used

The console port provides VT100 terminal emulation with the following parameter settings:

- ❒ Baud Rate: 9600
- ❒ Data bits: 8
- ❒ Stop bit: 1
- ❒ Parity: None
- ❒ Flow Control: None

Use the CLI commands

```
CONSOLE/SHOW
CONSOLE/CONFIG
```

to view and configure the console parameters. For information on these commands, refer to the *HiSpeed Switch User Guide*, document number US7070424-001, that was shipped with your switch.

Chapter 5
Fundamentals of Networking

Today, there are many different types of computers and networking equipment available. These devices are expected to communicate with each other. For this reason, it is extremely important that a set of rules be established and implemented in order for networking devices to function well together.

In 1978, the International Standards Organization (ISO) defined the Open System Interconnection (OSI) Model for networking. This reference model outlines the communications protocols used when transporting data from one network node to another. The standard was initially written to provide both hardware and software vendors a common platform on which to develop products. The model also serves as the basis for the IEEE LAN standards.

The OSI Model divides the task of computer communications into seven layers. The model represents a hierarchical structure and is designed so that each layer performs a specific service transparently to layer above and below it. In addition, the corresponding layers between two adjacent devices communicate to each other in a peer to peer relationship.

The Figure 5-1 shows the seven layers in the OSI Model in a peer-to-peer relationship

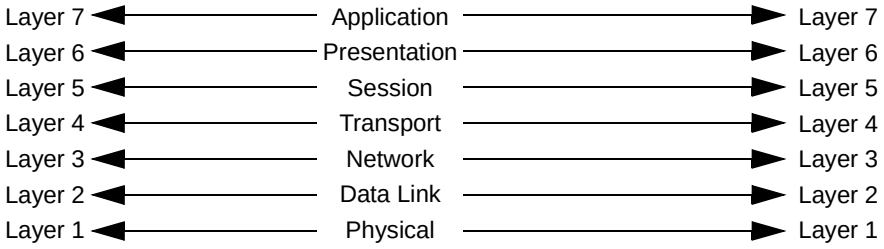


Figure 5-1. Network Media

Layers 1 through 3 define the network and how data is transferred across the network. Layers 4 through 7 define how the data is used. Each of the seven layers are described in more detail below.

Layer 1: Physical Layer

This layer defines the physical, mechanical, and electrical connection to the network. The Physical Layer is responsible for the actual transmission of the bit stream on the medium. Electrical issues such as voltage, current, frequency, and modulation techniques are governed by the physical layer.

Examples of Physical Layer specifications are cabling (10BASE5, 10BASE2, and 10BASE-T, 100BASE-T, etc.), type and size of the connector, number of pins in the connector, and the function of each of the pins.

Examples of Physical Layer devices are repeaters and hubs.

Layer 2: Data Link Layer

This layer is responsible for assembling and disassembling data into frames. The data link layer also checks the frames for error and flow control to ensure for reliable data transfer. The Data Link is subdivided into two separate sublayers: Media Access Control (MAC) and Logical Link Control (LLC).

The LLC sublayer defines the logical connection to the upper layer services based on a socket or Service Access Point (SAP). This allows two processes on the same network to maintain a "logical connection" with each other for the purpose of data exchange.

Examples of Layer 2 devices are bridges and switches.

Layer 3: Network Layer

This layer is where the network provides its routing functionality. The Network Layer uses a *packet* to transport data from one network to another. A 32-bit address is used to define the network's logical location and is referred to as the network address or IP address.

Examples of Layer 3 devices are routers.

Layer 4: Transport Layer

This layer ensures reliable delivery of data between networks. All error checking, acknowledgments, retransmissions, and data sequencing are handled by the Transport Layer.

Layer 5: Session Layer

This layer provides for the ability for two processes on two different stations to form a connection for the purpose of communication with one another. This is often referred to as a dialogue layer. Host-to-host communication is established, managed, and terminated at this layer.

Layer 6: Presentation Layer

This layer converts the actual data that is being transferred into a readable and proper form.

Layer 7: Applications Layer

This layer provides network-based services to a user's application. The application layer communicates with the end user via programs such as file transfers (FTP, TFTP), electronic mail (SMTP), and other applications.

Chapter 6
Methods of Managing the Switch

Hitachi's HiSpeed switch can be managed using the following:

- ❒ Serial connection on the console port
- ❒ Telnet session over a TCP/IP network
- ❒ SNMP using HiView's Graphical User Interface (GUI)

CLI (Command Line Interface)

Hitachi employes a command line interface (CLI) application for configuring the HiSpeed switch. The CLI can be accessed from:

- ❒ Console Port
- ❒ Telnet session

Using the Console Port

Connect a terminal to the HiSpeed switch using a null-modem RS-232 serial cable. A DOS/Windows or Unix workstation running in terminal emulation mode can also be used. The console port on the switch is configured as DCE, which requires the use of a null-modem cable. Because the connection is a male DB9 interface, your cable should be a female DB9 connector on the other end.

Configure the terminal to use the following parameters:

- ❒ Data bits: 8
- ❒ Stop bit: 1
- ❒ Parity: none
- ❒ Flow control:none

Troubleshooting a Console Connection

Use the following procedure to troubleshoot the situation when text will not display on the connected console:

1. Verify you are using a null modem cable.

   With a console cable, connect (2) PCs running a terminal application session and verify if both can send and receive text.

2. Check the terminal settings on your PC to match that of the switch.

   Default switch settings are: 9600, 8, 1, none, none

3. Check that your terminal or terminal emulator is correctly configured as VT100.
4. Restart your terminal session.
5. Check if there is a telnet session to the switch. If so, the following message appears:

   ```
   telnetd: This system *IN USE* via telnet.  You will then need to
   disconnect the telnet session.
   ```

6. Reset the switch if it is necessary.

Using a Telnet Session

The switch can be accessed from a remote location by using Telnet to make a TCP connection. The Telnet command syntax depends on the type of terminal or TCP/IP software you are using. Refer to your User Guide for Telnet instructions.

Telnet requires that your workstation is connected to the network with a valid IP address. In addition, you must know the IP address (or host name, if using a Domain Name Server) of the device you wish to connect to.

Troubleshooting a Telnet Session

Use the following procedure when you cannot establish a Telnet session to the switch:

1. Verify that the console setting on the switch is unlocked.

   ```
   /console>lock
   ```

2. Verify that a link is established on the Ethernet port.
3. Verify the port is enabled and in “Forwarding” mode. Using the CLI, type

   ```
   vvp
   ```

4. Ping yourself first. Verify the switch’s IP address, subnet mask, and the default router configurations are correct.

Logging In

The HiSpeed switch is shipped from the factory with pre-installed software. By default, the switch is configured to boot from flash. After the switch has been booted, the login prompt will be displayed. Log in by entering **admin**, in lowercase.

```
Login: admin
```

The switch will then prompt you for a password. Enter **switch**, in lowercase. The password will not be displayed on the screen. For security reasons, change the **admin** password as soon as possible. To do so, use the /SYSTEM/CONFIG/ADMINPW command. (Refer to the User Guide for more details on this command).

Troubleshooting the Login Procedure

Use the following procedure when you cannot log into the switch:

1. For console port access, press [Return] several times before the Login prompt appears.
2. Ensure that you are using all lowercase for your login name and password.
3. Contact your supplier to have your password reset if you are unable to log in with the correct password.

HiView Switch Management

The HiSpeed switch can be configured using Hitachi's HiView graphical user interface (GUI) application. HiView uses Simple Network Management Protocol (SNMP) to communicate to the SNMP agent residing on the switch. Configurations to the switch can be made easily by simply dragging and dropping icons from one window to another. The HiSpeed switch supports the following RMON groups: 1,2,3 and 9. A third party Network Management software is needed to probe the switch for statistics, history, alarms, and events. The following Network Management software have been tested with the HiSpeed switch:

- **SNMPC** by Castle Rock
- **MeterWare** by Technically Elite *(further testing needed for Hitachi's private MIBs)*
- **SNMPTalk** by Epilouge

However, any Network Management software will run on the HiSpeed switch.

HiView can be installed to run on both Windows 95/NT 4.0 and Unix platforms. Minimum system requirements are as follows:

Windows 95/Windows NT 4.0

The minimum system requirements to run under Windows 95/NT 4.0 are as follows:

- Pentium 133 Mhz processor
- 16 MB of memory
- 10 MB free disk space
- 1024 X 768 monitor resolution with 256 colors
- Microsoft (or compatible) mouse

UNIX

The minimum system requirements to run on a UNIX platform are as follows:

- ❒ Sun SPARC station
- ❒ SunOS 4.1.1 or later
- ❒ Motif 1.2 or greater
- ❒ OpenView X.X or later

Note: The HiSpeed switch must be running firmware version 1.3.9 or above.

HiView Tips

Windows 95/NT 4.0

- ❒ HiView can only manage one switch at a time.
- ❒ The default password for login is blank. Click on “OK” to initially launch the application. However, a password can be set at a later time.
- ❒ All fields for “Network Device Dialog Box” must be filled before launching the application.
- ❒ When the HiView application has been launched for the first time, the color on all Ethernet ports is black. To distinguish between different VLANs, you must assign different colors to the VLANs.
- ❒ To upgrade the firmware on the switch using HiView, a third party TFTP server process must be running.

HiView Tips

UNIX

- ❒ HiView can only manage one switch at a time.
- ❒ A login and password is not required for the Unix version of HiView.
- ❒ In the “Network Device Dialog Box”, only an IP address is required. The read/write community strings are defaulted to public/private.

- ❒ Select the VLAN prior to changing the VLAN color. Otherwise, a core dump will occur.

Troubleshooting HiView

- ❒ In the FDDI MAC statistics menu, the values for Frame Received and Frame Copied are different than CLI.
- ❒ When initially creating an ATM service from the CLI and modifying it from HiView, an error will error. It is recommended to create the ATM service from HiView.
- ❒ The LEC Arp does not contain any valid entries.
- ❒ One HiView License is allowed per device.

Troubleshooting Network Management software on the HiSpeed switch

SNMPC Issues

- ❒ For the RMON groups to work properly, do the following:
  1. Create table entries with [etherStatsStatus.x | historyControlStatus.x | alarmStatus.x eventStatus.x] equal to createRequest.
  2. Fill out the table entries with relevant values.
  3. Set the xxxStatus-field to valid.

Caution: Before changing any table entry values, set the stats-field to underCreation, change the values and set the xxxStatus to back to valid.

- ❒ In order to read the private MIBs via the SNMPC MIB browser, modify the definitions in the NSGTC.MIB.
  1. Open the NSGTC.MIB file with an ASCII text editor. The NSGTC.MIB is located in the \SNMPC\MIBFILES subdirectory.
  2. Find the IMPORTS header located at the top of the MIB file. Use a double hypen (--) to comment out the fields starting from "`hicamNsgConventions MODULE-IDENTITY" to`

“::= { enterprises hicam(399) nsg(2) nsgConventions(200) 1 }”. The following is an example of the modified section of the NSGTC.MIB.

EXAMPLE:

```
IMPORTS

    MODULE-IDENTITY, enterprises       FROM SNMPv2-SMI;

-- hicamNsgConventions MODULE-IDENTITY
--     LAST-UPDATED "9611082200Z"
--     ORGANIZATION "Hitachi Computer Products (America), Inc"
--     CONTACT-INFO
--             " Hitachi Computer Products (America), Inc
--               3101 Tasman Drive
--               Santa Clara, CA 95054
--               (401) 986-9770
--
--               support@spd.hitachi.com"
--     DESCRIPTION
--          "This module defines the top level object identifiers for
--             the HICAM Network System Group (NSG).  These object
identifiers
--           are imported by other internally developed MIB modules."
--     ::= { enterprises hicam(399) nsg(2) nsgConventions(200) 1 }
--

hicam          OBJECT IDENTIFIER ::= { enterprises 399 }
nsg            OBJECT IDENTIFIER ::= { hicam 2 }
```

Note: The information regarding the SNMPC mibs compiling procedure can be found on Technical Bulletin # US7110002-001

MeterWare Issues

For the RMON groups to work properly, do the following:

- ❒ Hitachi’s vendor id must entered to recognize the switch’s MAC address.
- ❒ Set the device to EthernetRMON.

Listed below are the steps to compile and browse Hitachi’s private MIBs with MeterWare:

1. Launch the MeterWare program.

2. Click on the menu bar labelled "*Tools*", then click on "*MIB compiler…*" A dialog windows will appear (see Figure 6-1).

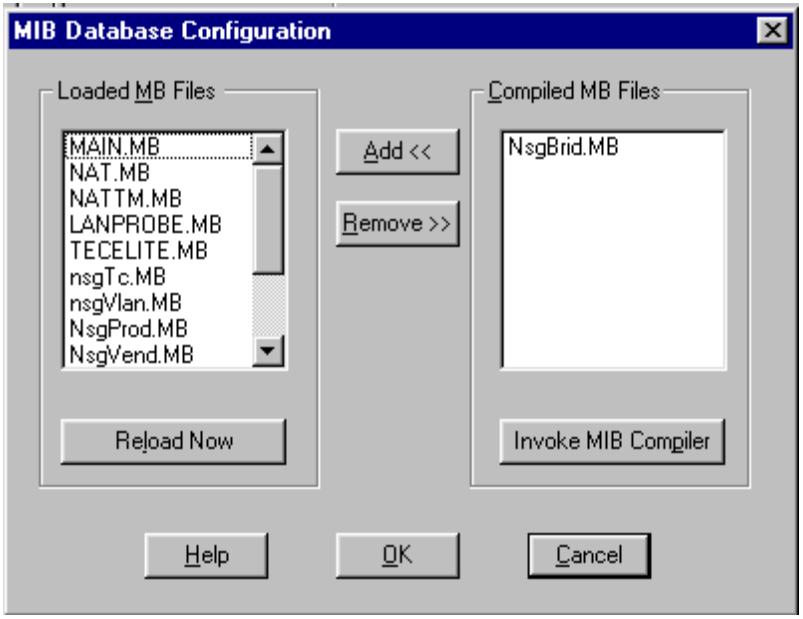


Figure 6-1. MIB Compiler

3. Click on "*Invoke MIB Compiler*", select the private MIBs to compile.

Note: The compiler will only compile one MIB at a time. Verify that all the compiled MIBs appear in the window labelled "*Compiled MB Files*".

4. From the "*Compiled MB Files*"list, select the MIBs to be added to the "*Loaded MB Files.*"list.
5. After all MIBs have been added, click on "*Reload Now.*" Then click on "OK".

Note: After initially clicking on "*Reload Now*", an error message will appear. Click on "*Reload Now*". Ignore the error message and click on "*Reload Now*"again.

6. Click on the menu bar labelled "*Tools*"and click on "*MIB Browser*". A dialog window will appear. See **Fig.2** below. Go to this directory :

   iso.org.dod.internet.mgmt. and click on *private (enterprises (hicam (nsg* .

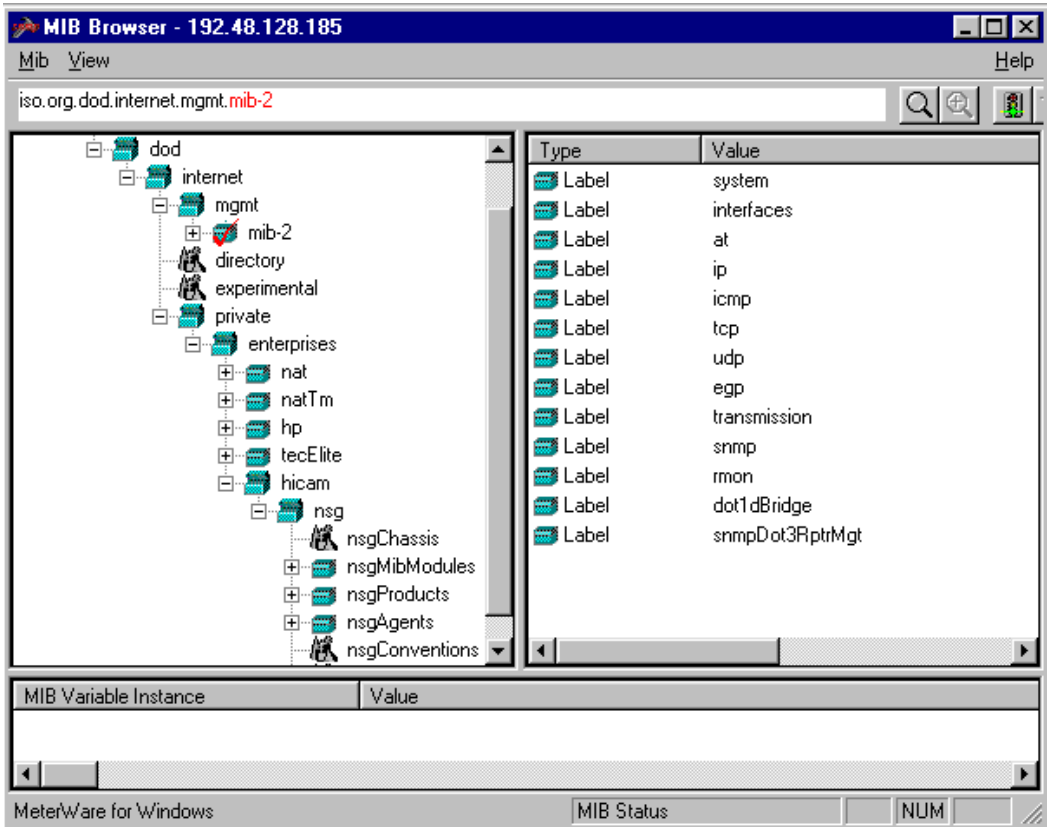


Figure 6-2. Fig2. MIB Browser

Note: Viewing Hitachi's private MIBs requires further testing.

SNMPTalk Issues

For the RMON groups to work properly, the `mib.rt` file needs to be loaded in the same directory as SNMPTalk. The `mib.rt` file contains all MIB information.

Chapter 7
Bridging Concepts

Basic Bridging Concepts

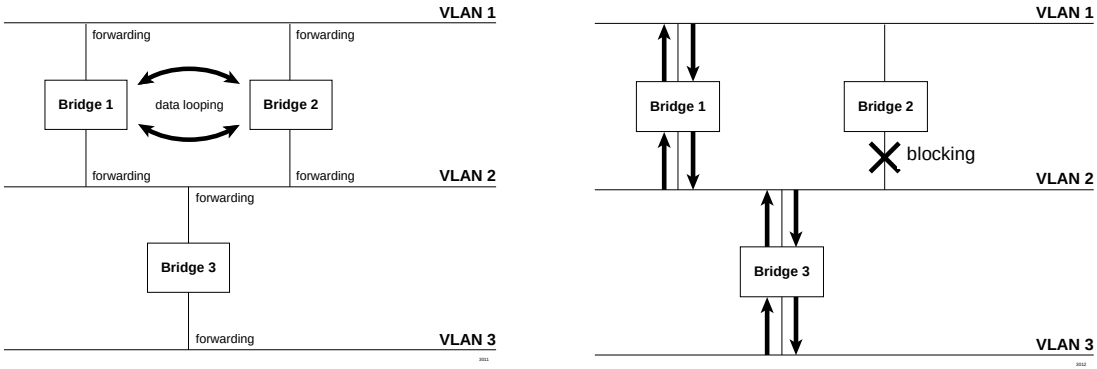
A bridge operates at the Data Link Layer of the OSI model by forwarding or flooding packets based on the destination MAC addresses. A bridge normally operates in promiscuous mode and learns all packets on the network. The bridge then builds an internal Forwarding table based on the source MAC addresses. When a bridge receives a packet, it compares the destination address with addresses in the Forwarding Table with one of the following results occurring:

- ❒ If the destination address is on the same LAN as its source address, the bridge will discard that packet.
- ❒ If the destination address is in the Bridge Forwarding Table, the packet will get forwarded onto the necessary port.
- ❒ If the destination address in NOT in the Bridge Forwarding Table, the packet will get flooded out all ports except the port on which the packet came in on. This also applies to broadcast, multicast and unknown unicast frames.

How Spanning Tree Works

Bridging loops occur when there are redundant bridge links in the network. To correct for this, the Spanning Tree algorithm is used to detect and prevent loops in the network. The version of Spanning Tree supported on the HiSpeed switches is IEEE 802.1D.

Spanning Tree is a configuration algorithm and protocol that ensures that no data loops exist within a single broadcast domain. Figure 7-1 shows bridges 1 and 2 in a loop; in this configuration without Spanning Tree, the network is unusable



Data looping

Using Spanning Tree to eliminate ata looping

Figure 7-1. Using Spanning Tree

When Spanning Tree is implemented, redundant bridge ports are blocked and looping is eliminated, as shown in Figure 7-1.

The first step in forming a Spanning Tree is electing a **root bridge**. Initially, each bridge assumes it is the root bridge for the LAN. Bridge Protocol Data Unit (BPDU) packets are sent onto each of its ports.

The bridge broadcasts BPDU packets and listens for BPDU packets from other bridges. The bridge compares each packet transmitted with each packet received. The root bridge is finally elected based on the following:

- ❒ Bridge with the Lowest Root ID. This is made up of a combination of the MAC address and bridge priority.
- ❒ If the root IDs are equal, the bridge compares the costs (least number of hops). To ensure maximum performance, the bridge will calculate the shortest path possible to get to the root bridge.
- ❒ If both the root IDs and the costs are equal, then the bridge compares the Transmitting Bridge ID's. The bridge will keep the frame with the lowest Transmitting Bridge ID.

If all of the parameters are equal, there is a final tie-breaker parameter known as the port identifier. Each port on a bridge has a port identifier, and the bridge will keep the BPDU frame with the numerically lower port ID.

If, on any given port, a bridge decides to keep a packet from another bridge instead of the packet that it would send, it no longer transmits BPDU messages. Basically, it drops out of the running because it realizes there is a better bridge for the job. When the algorithm finally stabilizes, only one bridge on each segment will transmit BPDUs on that segment. This bridge is known as the **designated bridge** for that segment.

Finally, the bridges decide which ports are active, and which are blocking. With Spanning Tree on, the ports go through the following Spanning Tree states:

- ❒ Listening
- ❒ Learning
- ❒ Blocking or Forwarding

Troubleshooting Bridging Issues

Problem: **PC is moved to a different port on the switch. Users can no longer ping me.**

Solution: Wait for Spanning Tree to stabilize completely. The default STA timer is 15 seconds for the ports to go from ‘Listening’ to a ‘Forwarding’ state. To verify the port state, type

```
vvp
```

You may also need to wait for the previous MAC entry to age out of the bridge forwarding table. The default bridge aging timer is 300 seconds. However, to expedite this process, ping the switch and it will immediately replace the previous MAC entry with the new one.
To view the Bridge Forwarding table, type

```
vfwt
```

Verify that a static entry has not been created for this user.
To show static entries, type ‘`fl`’
If so, you will need to remove that entry from the static table.
To delete a static entry, type

```
delfl
```

Problem: **After rebooting my PC, I cannot log onto my Novell or DHCP server.**

Solution: PCs equipped with faster processors will boot up before STA on the switch has completely stabilized. Because the ports on the switch have not gone to 'Forwarding', applications on the PCs may have timed out when trying to connect to the server.
To disable Spanning Tree on the switch, type

```
/VBRIDGE/CONFIG/bridge <vlan#>, select option 1
```

Note: Not recommended if there are redundant bridge paths resulting in loops on your network.

To reduce the STA timer, type

```
/VBRIDGE/CONFIG/bridge <vlan#>, select option 5
```

Note: Ensure that STA timers are set to be the same on all bridges. If BPDUs are transmitted at different time intervals, this may result in an unstable network (state of flux).

Problem: **The switch is constantly flooding the network with broadcast traffic. How can I control the amount of broadcast on my network?**

Solution: By design, a bridge will forward all broadcast traffic. However, if the switch is specifically broadcasting 'Unknown Unicast' packets, verify that DLF is enabled. The Destination Lookup Failure (DLF) mechanism slows down broadcasts sent from the CPU which may eventually consume total bandwidth on the network. By default, DLF is enabled. To enable/disable DLF on the switch, type

```
/VBRIDGE/CONFIG >throttle
```

If you have redundant bridge paths on your network, verify that STA is enabled and ports are in a forwarding/blocking state

```
/VBRIDGE/SHOW > bridge <vlan#>
/VBRIDGE/SHOW > port  <vlan#>
```

CLI Commands

`/vbridge/show/fwt`	Displays the bridge forwarding Table.
`/vbridge/show/filter/all`	Displays all static entries in the Bridge Forwarding Table.
`/vbridge/show/bridge <vlan#>`	Displays the bridge parameters per VLAN.
`/vbridge/show/port <vlan#>`	Displays the Spanning Tree port parameters per VLAN.
`/vbridge/config/bridge <vlan#>`	Modifies Spanning Tree parameters per VLAN
`/vbridge/config/filter`	Add/deletes static entries in the Bridge Forwarding Table.

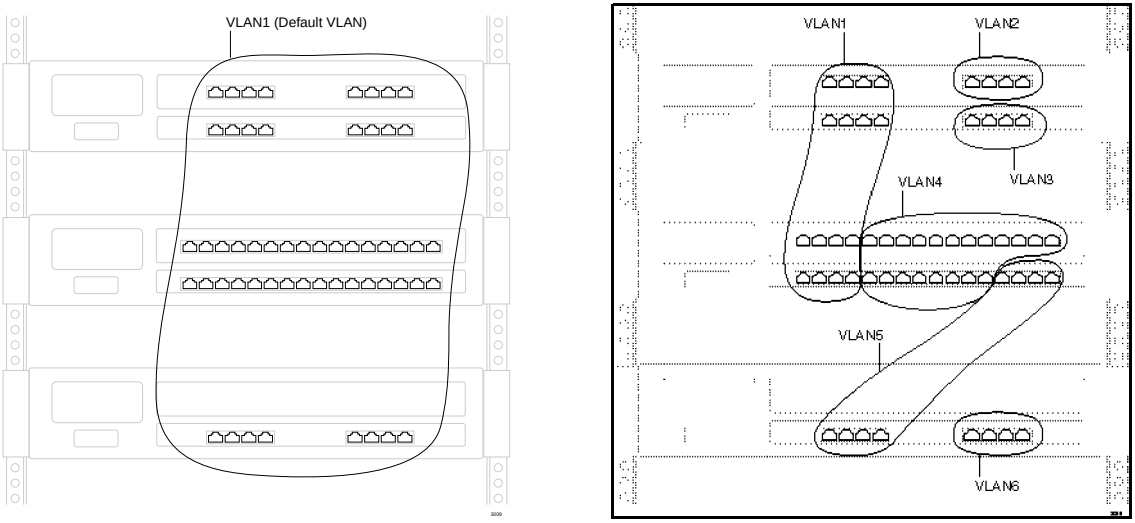
Chapter 8
VLAN Concepts

A VLAN is a network that logically divides workgroups by functions, applications, etc. without regards to the physical location of users, thereby localizing network traffic to those you would communicate with most often. VLANs are bounded by routers, therefore, data within a VLAN does not leave the VLAN without routing.

The HiSpeed switch uses IP routing to forward packets across different VLANs. Routing must be enabled per VLAN and assigned an IP address. When routing is enabled, a Virtual Router port is created and traffic is routed onto the VLAN via that Virtual Router port.

Note: The HiSpeed switch is pre-configured with a default VLAN 1. In order to route between VLANs, you must either connect an external router to the switch or enable IP routing per VLAN.

The HiSpeed switch implements VLANs on a per port(s) basis. Ports assigned to a VLAN share the same broadcast whereas ports not belonging to that VLAN are not part of that broadcast domain. By separating groups into different VLANs, overall network performance is improved. Unlike rule-based VLANs, multiple VLANs do not share the same physical segment (or switch port(s)).



Default VLANs **Multiple VLANs**

Figure 8-1. VLANs

VLANs provide some of the following benefits:

- ❒ Reduced costs

  As a company grows and reorganizes, physical moves, adds, and re-cabling are made to their network. VLANs provide a cost effective solution to network changes. Because VLANs are location independent, adds and moves are quickly accomplished without the need to rewire the physical infrastructure.

- ❒ Better security

  VLANs offer security by logically separating groups by departments, functions, etc., therefore, limiting and/or restricting user access and priviledges to specific applications and resources.

- ❒ Efficient use of network bandwidth

  VLANs maximize the efficient use of bandwidth on any given LAN segment, since packets are forwarded only between segments as required. In addition, VLANs create smaller broadcast domains which reduce the amount of broadcast traffic across the entire network.

Troubleshooting VLANs

Problem: **Cannot ping a user(s) on a different VLAN.**

Solution: Verify the following:

- Verify that the port(s) the user(s) is connected to has the correct VLAN number(s) assigned to it.

  ```
  /VLAN/SHOW >vlan
  ```

- Verify that you can ping the switch itself. By default, the switch is not pre-configured with an IP address. Therefore, you must enable IP and assign an address to it.

  ```
  /VLAN/CONFIG >modify  <vlan#>
  /VLAN/CONFIG >create <vlan#>
  ```

- Verify that the user endstation(s) and the VLAN(s) on the switch are using the same subnet masks.

  ```
  /VLAN/SHOW >vrouter
  ```

- Verify that the gateway IP address(es) on the endstation(s) points to the IP address of the VLAN(s) it is connected to.

- Check the ARP table on the switch to verify if the switch is learning the endstation(s) address(es).

  ```
  /INET/SHOW >ARP
  ```

- Check the Routing table on the switch to verify that all networks are learned.

  ```
  /INET/SHOW >route
  ```

- Check the Forwarding table to verify the correct MAC addresses are learned.

  ```
  /VBRIDGE/SHOW >vfwt
  ```

- Ping from the switch to the end nodes.

- Ensure that RIP is active per VLAN.

  ```
  /VLAN/CONFIG >modify <vlan#>
  ```

VLAN Tips

For each VLAN created with an IP address, an associated entry is also generated. Therefore, it is critical to verify that these entries exist. If any of the entries are missing, the system configuration may be corrupted. It is recommended to delete and re-create the VLAN.. Table 8-1 lists the VLAN entries and Table 8-2 lists useful CLI commands.

Table 8-1. VLAN Entries

Description:	CLI command:	VLAN entry created:
Virtual Port Information table	`/VLAN/SHOW >vport`	Router Virtual Port id '33'
Bridge Forwarding (ARL) table	`/VBRIDGE/SHOW >fwt`	MAC entry with Port id '33'
Routing table	`/INET/SHOW >route`	Route entry with a directly connected VLAN Interface type

Table 8-2. Useful CLI Commands

/VLAN/SHOW >vlan	Displays the VLAN information.
/VLAN/SHOW >vstats	Displays all Virtual Port statistics.
/VLAN/SHOW >vport	Displays all Virtual Port information.
/VLAN/SHOW >vrouter	Displays all Virtual Router information.
/VLAN/CONFIG	The following subcommands are available for VLAN configuration: • ADDPORT • CREATE • DELPORT • DIABLE • ENABLE • MODIFY • MOVPORT • REMOVE

Chapter 9
Troubleshooting at the MAC Layer

Ethernet

Ethernet is a LAN based technology with data transmission rates of 10 or 100 Mbps. CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol dictates how Ethernet frames traverse the network. In CSMA/CD, an Ethernet station checks for the presence of a signal on the cable. If there is no signal, the station begins transmission. However, more than one station can sense an idle channel and simultaneously begin to transmit data resulting in a collision. When this occurs, all stations involved detect the collision and immediately stop transmitting. After waiting a random time interval and ensuring that the line is free, each station will retransmit. If another collision occurs, the station must wait another random time interval before attempting to retransmit. After 16 tries, the station reports that the network is unavailable and discards the frame.

Based on the CSMA/CD methodology, collisions are inherent to Ethernet and considered ‘normal’. Retransmit delays due to collisions usually go unnoticed by the users, however, on larger networks with hundreds of users, excessive collisions may cause slow response times. Segmenting the network into smaller collision domains should significantly improve network performance.

Physical Media Specifications

	10BASE-5 (Thick Coaxial cable)	10BASE-2 (Thin Coaxial cable)	10BASE-TX (Unshielded Twisted Pair-UTP)	10BASE-FX (Fiber Optical Link)
Max. stations per segment	1024	1024	1024	1024
Max. segment length	500 meters	185 meters	100 meters	200 meters
Connector type	DB15 AUI	BNC	STAR	STAR
Cable type	RG-11	RG-58	Cat 3 or 5	62.5/125 mm or 9/125 sm

Common Ethernet Errors

collisions	Occurs when more than one device is transmitting simultaneously. Collisions are considered to be ‘normal’ in an Ethernet environment. CSMD/CD is designed to detect and correct for this.
late collisions	A collision detected after 64 bytes have been transmitted. May indicate a malfunctioning NIC/cable, or a network segment that has exceeded the maximum length.
excessive collisions	The maximum number (16) of consecutive collisions allowed between endstations contending for the wire. Possibly caused by exceeding the maximum number of users on a given segment, length of cable, or jabbering NIC.
undersized frames/ runts	Frames smaller than the minimum Ethernet frame size of 64 bytes a.k.a. ‘runts’. Presumed to be a fragment resulting from a collision.

alignment errors	Frame that contains a total number of bits not divisible by eight and fails the checksum test. This failure may be a result of collision, a defective NIC, bad cabling, etc.
oversized frames	Frame greater than the maximum Ethernet frame size of 1518 bytes. This failure may be caused by jabbering or defective devices in the network. Can cause FIFO buffer overflow, collisions, fragments, CRC, or alignment errors.
FCS errors	Generated when the CRC value on both the sending/ receiving stations are not identical. This value is calculated to verify the data integrity of the packet. If the receiving station recalculates the CRC and the value is not the same, the packet is discarded.
dribble bits	As a result of a transmitter (MAC) with poor timing.

Ethernet Tips

- Ensure that both port speed and duplexity on the switch and endstations are the same.
- By default, autonegotiation is enabled on the switch. If the endstation's network adapter card is not autonegotiating properly, disable autonegotiation on the switch and manually configure the port settings using the following command:.

```
/ETHERNET/CONFIG >port
```

Troubleshooting Ethernet

Problem: **Switch is not reporting any port statistics even with traffic on my network.**

Solution: By default, port statistics is disabled on the switch.

```
/ETHERNET/CONFIG >stat
```

Note: Enabling stats may cause a slight degradation to performance on the switch.

Problem: **Network is experiencing a large number of packet losses..**

Solution: The following solutions apply:.

- Port settings are set properly on the switch.

  ```
  /ETHERNET/CONFIG >port
  ```

- Check the Ethernet error statistics on the switch and take corrective action. (Refer to ‘Common Ethernet errors’ matrix for possible causes). More than likely, there is a physical layer problem caused by bad cabling, malfunctioning NIC, etc. In most cases, packets will be dropped by the switch due to excessive collisions, late collisions, FCS, alignment errors, oversized and undersized frames.

  ```
  /ETHERNET/SHOW >count <port#>
  ```

- Transmit and receive queues can get full when the switch port is oversubscribed with traffic. Check the ‘discBuffFull’ and ‘discMemFull’ counters and verify if they are incrementing.

  ```
  /ETHERNET/SHOW >count <port#>
  ```

  To clear the buffer queues:

  ```
  /ETHERNET/CONFIG/FLUSH >PORTFLUSH <port#>
  /ETHERNET/CONFIG/FLUSH >ALLPORTFLUSH
  ```

CLI Commands

`/ETHERNET/SHOW >port`	Displays all port speeds, duplexity, autonegotiation.
`/ETHERNET/SHOW >stat`	Displays if Ethernet statistics are enabled/ disabled on a per port basis.
`/ETHERNET/SHOW >count <port#>`	Displays tx/rx statistics & Ethernet errors on a per port basis.
`/ETHERNET/SHOW >macaddrcount`	Displays the total count of MAC source address entries in the Bridge Forwarding Table.
`/ETHERNET/CONFIG >clear <port#>`	Resets the port statistic counts to zero.
`/ETHERNET/CONFIG >port`	Configures the port speed, duplexity, autonegotiation.
`/ETHERNET/CONFIG/FLUSH >portflush <port#>`	tbd
`/ ETHERNET/CONFIG >stat <port#>`	Enables/Disables Ethernet statistics on a per port basis.

Chapter 10
Troubleshooting at the Network Layer

IP (Internet Protocol)

The HiSpeed switch supports IP (Internet Protocol), a widely used Network Layer protocol used by devices to communicate across a network. IP utilizes a 32-bit address structure to identify the network and node number. The three primary classes of IP addresses are as follows:

Table 10-1. IP address classes

Class	Range:	Subnet Mask:
Class A	0 - 127	255.0.0.0
Class B	128 - 191	255.255.0.0
Class C	192 - 223	255.255.255.0

Note: 127.0.0.1 is reserved for loopback testing.

Other IP-related Services

The HiSpeed switch supports the following IP-related functions:

- Address Resolution Protocol (ARP)
  Used to resolve an IP to MAC address allowing devices to communicate at the Data Link layer. The HiSpeed switch maintains an ARP table of IP to MAC address mappings.
- Internet Control Message Protocol (ICMP)
  Provides a mechanism allowing a device to report an error back to the original source. Ping packets which employ ICMP, are used to determine whether a device is reachable across the network.
- TCP (Transmission Control Protocol)
  Used by applications requiring a reliable transport mechanism for communicating between devices across the network. Examples of network applications using TCP are: Telnet, FTP, SMTP.
- UDP (User Datagram Protocol)
  Used by applications that do not require a reliable transport mechanism for communicating between devices across the network. Examples of network applications using UDP are: DNS, TFTP, SNMP.

RIP (Routing Information Protocol)

The HiSpeed switch uses RIP, version 1, to route IP packets across VLANs. RIP, a distance vector protocol, computes the best path to the destination based on the least number of hops. If more than one path exists with the same metric, the switch will choose whichever path it first learns.

An internal Routing table based on network address, gateway, metric, VLAN, and Interface type is built and maintained on the HiSpeed switch. These routes are propagated across the network via RIP every 30 seconds. Without RIP updates, dynamic routes age out after 180 seconds. The maximum number of RIP entries supported on the HiSpeed switch is 512.

To prevent routing loops, the HiSpeed switch implements **Split Horizon. N**etworks that are learned through a particular interface will not get advertised back out that same interface.

Note: RIP version 1 does not propagate subnets. RIP assumes that the same subnet mask is used throughout the entire network, therefore, ensure subnet masks are identical.

Route Cache Forwarding vs. IP Forwarding

The HiSpeed switch provides a fast data path for forwarding IP packets called Route Cache Forwarding. Only TCP/UDP traffic over IP is supported. To forward packets at a higher speed, a cache is maintained to store IP addresses and Layer 2 information. An entry is created for each communicating pair of IP addresses. Once a route is learned, traffic destined for the port will be forwarded directly to the interface without going through the IP Forwarding mechanism.

Tip: The Route Cache table can store up to 1024 routes and has an aging timer of five minutes. Currently, there is no mechanism for invalidating routes if there is an address or port change. Traffic will still be forwarded to the previous port. To continue to use the Route Cache feature, you must wait for the old entry to age out.

Static Routes vs. Dynamic Routes

Static routes are manually configured while dynamic routes are learned. Unlike dynamic routes, static routes never age out. To remove a static route, it must be manually deleted from the routing table.

Default Route

An address of `0.0.0.0` signifies a default route used for all unknown networks. Typically, the default route points to a router which maintains a complete routing table. A default route is commonly used on a router as an entry point to the Internet. Defining a default route on the HiSpeed switch allows the switch to forward packets to unknown destination networks via an external router.

Common ICMP Destination Unreachable Messages

Network Unreachable

This message is sent by a router indicating that it cannot reach the specified network. This may be a result of a misconfigured mask, link down, missing route, or an invalid network.

1. Is the specified destination address a valid network?
2. Is the link up from the router sending the Network Unreachable message?
3. Is the port in the router configured with the correct subnet mask?
4. Does the route exist in the routing table?

Host Unreachable

This message is sent by a router indicating that the destination host did not respond. The significance of this implies that the intervening network infrastructure is working properly and the frame has successfully arrived at the last router in the path. The ARP request to the destination host did not respond. This may be a result of a user typing an incorrect IP address or a high number of physical layer errors on the destination network.

1. Is the destination IP address correct?
2. Is the destination host available?
3. Are there any physical layer problems on the destination network?
4. Is the default gateway correctly defined on the destination device?
5. Verify that the destination device can ping its default gateway. From the ARP table of the destination device, is the default gateway address learned?

Port Unreachable

This message is sent by the destination host device indicating that the port process is not functioning properly or does not exist. One of the most common Port Unreachable errors occurs when an SNMP manager is polling a device on the network which didn't have an SNMP agent configured on it.

1. Is the port process enabled or running?
2. Find out what the port is used for and why isn't it available. Refer to RFC 1700 for a complete list of well-known ports.

Troubleshooting IP

Problem: A**n external router is connected to my switch. I can ping the router interface on my network but cannot reach any networks beyond the router.**

Solution: Use the following solutions:

- Verify that the gateway IP address(es) on the endstation(s) points to the IP address of the VLAN(s) it is connected to. Also, verify that your own IP address and that of the end station you are trying to connect to is correct
- Ensure that RIP is active per VLAN.

  ```
  VLAN/CONFIG >modify <vlan#>
  ```

- Check the Routing table on the switch to verify that all networks are learned. If not, you may need to configure a default route of 0.0.0.0.

  ```
  /INET/SHOW >route
  /INET/CONFIG/ROUTE >default
  ```

- Verify that the user endstation(s) and the VLAN(s) on the switch are using the same subnet masks.

  ```
  /VLAN/SHOW >vrouter
  ```

- Check all router interfaces to ensure they are up and active.
- Verify that the HS150 port is in the correct VLAN.

  ```
  /VLAN/SHOW >vlan
  ```

- Check broadcast address on the router to verify that it is the same as the end node expects. On the HiSpeed switch, type:

  ```
  /VLAN/CONFIG >modify <vlan#>
  ```

Problem: **Performance is slow when routing across different networks.**

Solution: Use the following solutions:

- By default, IP Forwarding is enabled on the switch. Configure the switch for Route Cache Forwarding.

  ```
  /INET/CONFIG/ipr
  ```

- and performance issues. If using static routes on the HiSpeed switch, you must configure those routes on those directly connected switches and routers. On the HiSpeed switch, use the following command:

```
/INET/SHOW >static
/INET/CONFIG/ROUTE/add
```

Problem: **Cannot establish a telnet session to the switch.**

Solution: The HiSpeed switch uses the well known TCP port 23 for Telnet. Verify that the socket is in a 'Listen' state.

```
/INET/SHOW >iconnect:
```

CLI Commands

`/INET/CONFIG/ipr`	Enables/disables Route Cache Forwarding.
`/INET >ping <hostname> [NumberofPackets]`	Performs an ICMP echo request.
`/INET >rlogin <hostname>`	Used when logging onto a Unix server.
`/INET/CONFIG/ROUTE >` • ADD • DEFAULT • DELETE • RMDEFAULT	Commands available for configuring static and default routes.
`/INET/SHOW >` • ARP • ROUTE • STATIC • ICONNECT • RTCACHE	Commands available for displaying Routing tables, ARP cache, and TCP/IP connections.
`/INET >stats` • FORWARD • ICMP • IP • SNMP • TCP • UDP	Commands available for displaying IP statistics.

Chapter 11
Basic ATM Concepts

Asynchronous Transfer Mode (ATM) is a connection-oriented protocol using 53 byte fixed length cells. One significant advantage of ATM is the ability to carry voice, video and data traffic simultaneously over a 155 megabit per second pipe. The Hitachi HiSpeed switch is an ATM edge device and provides Ethernet to ATM connections over an ATM network.

Within the physical link, each Virtual Channel Connection (VCC) is uniquely identified by VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) pairs. The VPI/VCI identifiers allows the network to associate each cell with a virtual path and channel to switch data through. Each VPI/VCI pair has local significance only allowing identical VPI/VCI combinations to exist on different interfaces within the network.

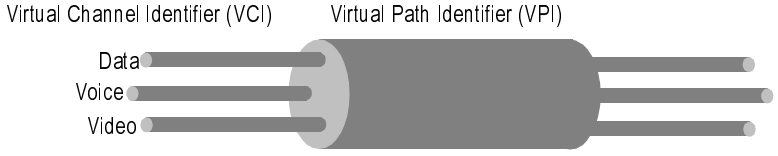


Figure 11-1. VPI/VCI

Permanent Virtual Circuits vs. Switched Virtual Circuits

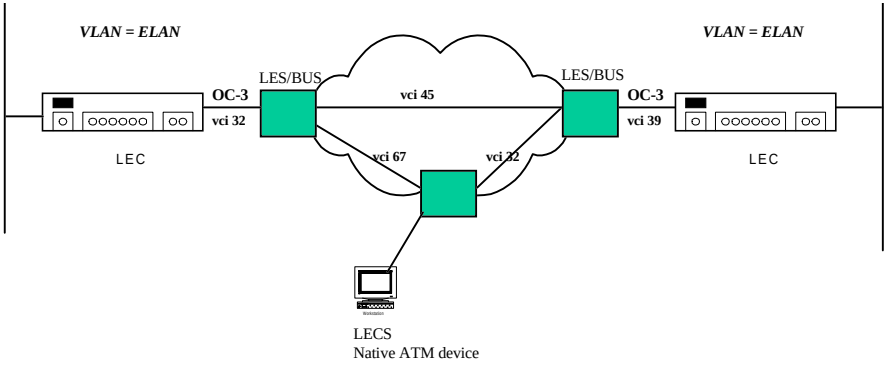
ATM connections can be established manually (Permanent Virtual Circuits) or dynamically (Switches Virtual Circuits). Permanent Virtual Circuits (PVCs) are usually defined for long-term connections and automatically re-established after a network failure. Switched Virtual Circuits (SVCs) uses **Q.2931** signaling to define and release connections as needed. Unlike PVCs, SVC connections are not automatically re-established after a network failure.

The HiSpeed switch implements the following ATM services:

- ❒ LAN Emulation (LANE)
- ❒ Classical IP over ATM (CIP)
- ❒ Point-to-Point Bridging (PTOP)
- ❒ Trunking

LAN Emulation (LANE)

LANE emulates a traditional LAN (ie. Ethernet or Token Ring) over ATM by mapping MAC addresses to ATM addresses, connectionless technologies to connection-oriented technologies, and emulating the broadcast nature of LANs.



**** Every ELAN must have (1) unique LES/BUS pair.***
***** Valid LEC values range from 0 through 31.***

Figure 11-2. ATM LANE

The components of an Emulated LAN (ELAN) consists of the following:

- ❒ LAN Emulation Client (LEC)
- ❒ LAN Emulation Configuration Server (LECS)
- ❒ LAN Emulation Server (LES)
- ❒ Broadcast and Unknown Server (BUS)

LAN Emulation Client (LEC)

The LAN Emulation Client (LEC) resides on the HiSpeed switch and acts as a proxy for devices connected to the Ethernet ports. In addition, the LEC responds to any LAN Emulation Address Resolution Protocol (LE_ARP) requests from host machines on the network.

LAN Emulation Configuration Server

The LAN Emulation Configuration Server (LECS) provides the LEC with the ATM address of the LAN Emulation Server (LES) to join an ELAN. It also provides the LEC with configuration information. The LEC can connect to the LECS in one of three ways:

- ❒ Use ILMI
- ❒ Use the LECS well-known address:
  `47007900000000000000000000:00A03E000001:00`
- ❒ Use a Config Direct VCC of 0.17 (one for each ELAN)

LAN Emulation Server (LES)

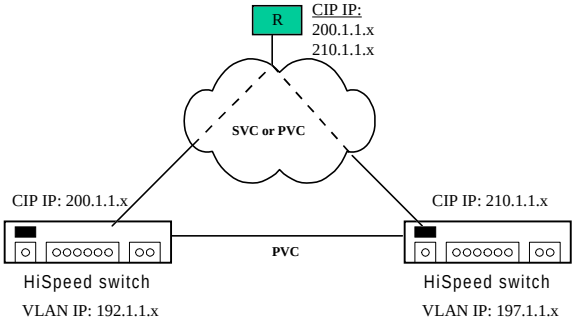
The LES registers and resolves MAC addresses to ATM addresses within the ELAN. The LES forwards the LEC response and helps the LEC locate the BUS, by responding to the LE_ARP request from the LEC.

Broadcast and Unknown Server (BUS)

The BUS forwards all broadcasts, multicast and unknown unicast traffic to all attached LAN Emulation Clients (LECs).

Classical IP over ATM (CIP)

Classical IP (CIP) allows devices in different IP subnets to communicate across an ATM network. If the Classical IP (CIP) interfaces are on different LIS (Logical IP subnets), and an external router is required. However, if the Classical IP (CIP) interfaces are on the same IP subnet, an external router is **not** required. Clients use the ATM ARP Server to obtain IP to ATM address mappings for end nodes in the Logical IP Subnets (LIS).

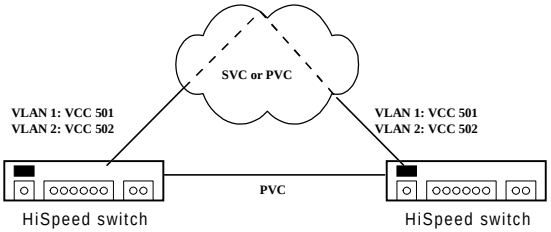


**To route between different Logical IP subnets (LIS) over CIP, an external router is required.*
***To route on the same Logical IP subnet (LIS) over CIP, an external router is **not** required.*
****When configuring PVC connections through an ATM switch, ensure the bi-directional path is established per port/interface on the ATM switch.*
*****CIP IP addresses must be on different subnets than those existing on the HiSpeed switches.*
******Valid CIP index ranges from 0 through 31.*
*******When configuring PVC, valid VCI values begin with 32.*

Figure 11-3. ATM CIP

Point-to-Point Bridging (PTOP)

Point to Point Bridging (PTOP) allows devices on the same IP subnet to communicate across ATM. Because VLAN information is not propagated across ATM, only one VLAN can communicate on a single virtual channel connection (VCC). PTOP can either use Permanent Virtual Connections (PVCs) or Switches Virtual Connections (SVCs).

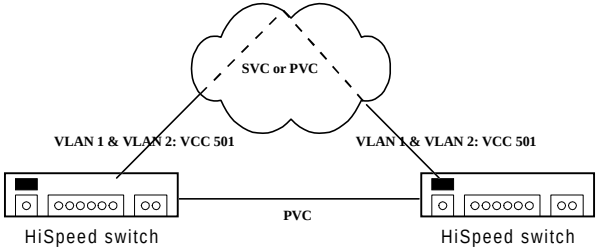


**When configuring a SVC connection, ensure the correct PTOP indexes are mapped to the switch you are connecting to.*
***When configuring a PVC connection, ensure the VCI values are identical on the switches you are connecting to.*
**** When configuring PVC connections through an ATM switch, ensure the bi-directional path is established per port/interface on the ATM switch.*
*****Valid PTOP index ranges from 0 through 15.*
******When configuring PVC, valid VCI values begin with 32.*

Figure 11-4. ATM PTOP

Trunking

Trunking allows multiple VLANs to share the same virtual channel connection (VCC) using either Permanent Virtual Connections (PVCs) or Switched Virtual Connections (SVCs). Unlike PTOP, VLAN information is passed across ATM thereby simplifying configuration.



**When configuring a SVC connection, ensure the correct PTOP indees are mapped to the switch you are connecting to.*
***When configuring a PVC connection, ensure the VCI values are identical on the switches you are connecting to.*
**** When configuring PVC connections through an ATM switch, ensure the bi-directional path is established per port/interface on the ATM switch.*
*****Valid Trunk index ranges from 0 through 31.*
******When configuring PVC, valid VCI values begin with 32.*

Figure 11-5. ATM Trunk

Hitachi HiSpeed ATM Specifications

- ❒ UNI 3.0 & 3.1 signaling is supported.
- ❒ Conforms to ILMI Registration 3.1 and ILMI MIB 4.0 specifications.
- ❒ Due to memory constraints over the ATM uplink, 16 is the recommended number of PTOP, Trunk, CIP, and LEC instances allowed under heavy traffic load.
- ❒ One LEC per ELAN is recommended.
- ❒ The HiSpeed switch does not support QOS (Quality of Service) parameters. Traffic management on the switch is UBR only.
- ❒ The maximum number of VCCs supported is 1024

ATM Troubleshooting Tips

- ❒ The ATM uplink module must be inserted into the lower PCI slot only.
- ❒ A multimode fiber (MMF) cable is required for use with the 155 Mbps ATM uplink OC-3 module.
- ❒ Bind LANE, PTOP, and Trunking services via the port service command. ***/portserv/config/create 34***
- ❒ Enable ILMI for LANE and signaling.
- ❒ Employ an external router for communication between logically separate ELANs for CIP.
- ❒ Every ELAN must have one unique LES/BUS pair for LANE.
- ❒ To join a specific ELAN, an ELAN name must be defined.
- ❒ Ensure the same UNI signaling version is used between the ATM edge devices and the ATM switch.
- ❒ When manually entering the ATM address of the switch, omit the AFI prefix (Ox).
- ❒ Valid Trunk Indexes range from 0 through 15.
- ❒ A VCI value is required when configuring PVC connections. Valid VCI values range from 32 to 1023 (0-31 are reserved by the ATM Forum).

- ❒ If your ATM configuration is corrupt, delete your ATM file from the CLI *(rm atm.cur)*, reset the switch, and re-configure ATM.
- ❒ Signaling changes may require you to reboot the switch.

Troubleshooting LANE

Problem: **I've created a LEC service but still cannot connect to the ATM network.**

Solution: Use the following solutions:

- Verify the LEC has been created, admin status is enabled, and protocol state is 'active'. Use the following command:

  ```
  /ATM/SHOW/lec <lec id>
  /ATM/CONFIG/ENABLE/lec <lec id>
  ```

- Ensure that you are using a valid LEC id. Valid LEC values ranges from 0 through 31

  ```
  /ATM/CONFIG/CREATE/lec <lec id>
  ```

- Ensure the ATM port is configured for SVC mode and ILMI is enabled. By default, the ATM port is set to 'PVC' mode and ILMI disabled.

  ```
  /ATM/CONFIG/MODIFY> port
  ```

Problem: **The LEC connection is up and active but I cannot ping across the ATM network.**

Solution: Use the following solutions:

- Verify that all IP addresses, subnet masks, gateways are set correctly on the VLANs and any attached devices.
- Verify that the ATM port service has been bound to each VLAN.

  ```
  /PORTSERV/CONFIG/create 34
  vps 34
  ```

- Verify all ATMLANE ports are in a 'Forwarding' state using vvp
- Depending on Spanning Tree, this process may take up to 20 seconds.

Troubleshooting CIP

Problem: **I've created a CIP service but still cannot connect to the ATM network.**

Solution: Use the following solutions:

- Verify that the CIP service has been created, admin status is enabled, and protocol state is 'active'.

  ```
  /ATM/SHOW/cip  <cip id>
  /ATM/CONFIG/ENABLE/cip <cip id>
  ```

- If using SVC connections, ensure that the ATM port is configured for SVC mode and ILMI is enabled. By default, the ATM port is set to 'PVC' mode and ILMI is disabled.

  ```
  /ATM/CONFIG/MODIFY> port
  ```

- If using SVC connections, ensure that you are using the same UNI signaling version as that of the connected ATM switch.

  ```
  /ATM/CONFIG/MODIFY >port
  ```

- If using SVC connections, ensure that you are using the same UNI signaling version as that of the connected ATM switch.

  ```
  /ATM/CONFIG/MODIFY >port
  ```

- If using SVC, verify that the ATM address of the ARP Server is correct. Also, verify the ARP Server is up and active on the switch you are connecting to.
- Verify the following using `/ATM/SHOW/connection`:
  - OAM is up.
  - SSCOP, and ILMI is up. *(for SVC only)*
  - A CIP SVC or PVC connection is created per CIP instance.
  - ATM port connection and signaling. Operational status, Line state, Signaling status, and ILMI should be 'up'. (for SVC only)

    ```
    /ATM/CONFIG/MODIFY> port
    ```

- Verify the connection up time is increasing and status is 'active' for a specific VCC using `VAC <VCC number>`

Problem: **The CIP connection is up and active but I cannot ping across the ATM network.**

Solution: Use the following solutions:

- Verify that all IP addresses, subnet masks, and gateways are set correctly on the VLANs and any attached devices
- Verify the same subnet mask is being applied to the CIP and VLAN interfaces.

  ```
  /ATM/SHOW >cip <cip id>
  /VLAN/SHOW/router
  ```

- Verify any of the CIP IP addresses must be on a different IP subnet than those VLANs existing on the HiSpeed switches.

  ```
   /ATM/SHOW >cip <cip id>
  /VLAN/SHOW/vlan
  ```

- Verify the VLANs communicating with one another over ATM belong to different IP subnets. VLANs belonging to the same IP subnet are not allowed to communicate with one another via CIP.

  ```
  /VLAN/SHOW/VLAN
  ```

- If using PVC, verify the VCI values are identical on the HiSpeed switches. However, the CIP index does not need to be the same on both switches.

  ```
  /ATM/SHOW >cip
  ```

- Verify that RIP is active for CIP and verify all routes are being learned.

  ```
  /ATM/SHOW >cip <cip id>
  /INET/SHOW >route
  ```

Troubleshooting PTOP

Problem: **I've created a PTOP service but cannot connect to the ATM network.**

Solution: Use the following solutions:

- Verify that the PTOP service has been created, admin status is enabled, and protocol state is 'active'.

  ```
  /ATM/SHOW/ptop  <ptop id>
  /ATM/CONFIG/ENABLE/ptop  <ptop  id>
  ```

- If using SVC connections, ensure that the ATM port is configured for SVC mode and ILMI is enabled. By default, the ATM port is set to 'PVC' mode and ILMI is disabled.

  ```
  /ATM/CONFIG/MODIFY> port
  ```

- using SVC connections, ensure that the ATM port is configured for SVC mode. By default, the ATM port is set to 'PVC' mode.

  ```
  /ATM/CONFIG/MODIFY> port
  ```

- If using SVC connections, ensure that you are using the same UNI signaling version as that of the connected ATM switch.

  ```
  /ATM/CONFIG/MODIFY >port
  ```

- If using SVC connections, verify the following:
  - Port configured as SVC, ILMI enabled, and the UNI version is correct.

    ```
    /ATM/CONFIG/MODIFY >port
    ```

  - Correct ATM address of destination switch. The last 2 selector bytes needs to be configured as follows:

    Example: `xxx52`

    `'xxx'` denotes the ATM address defined on the switch. Do a 'vap' to find out what it is.

    `'5'` is a reserved identifier for PTOP.

    `'2'` identifies the PTOP index configured on the destination switch.

  - Ensure the correct PTOP index is mapped to the switch you are trying to connect to.

  - Verify signaling and ILMI status should be ‘up’.

    ```
    /ATM/SHOW >port
    ```

- Verify the following using `/ATM/SHOW/connection:`
  - OAM is up.
  - SSCOP, and ILMI is up. (for SVC only)
  - A Pt-Pt SVC or PVC connection is created per PTOP instance.
  - ATM port connection and signaling. Operational status, Line state, Signaling status, and ILMI should be ‘up’. *(for SVC only)*

    ```
    /ATM/CONFIG/MODIFY> port
    ```

- Verify the connection up time is increasing and status is ‘active’ for a specific VCC using `VAC <VCC number>`

Problem: **The PTOP connection is up and active but I cannot ping across the ATM network.**

Solution: Use the following solutions:

- Verify that all IP addresses, subnet masks, and gateways are set correctly on the VLANs and any attached devices
- Verify the ATM port service has been bounded to each VLAN.

  ```
  /PORTSERV/CONFIG/create 34
  vps 34
  ```

- Verify all ATMPTOP ports are in a ‘Forwarding’ state using vvp

Note: Depending on Spanning Tree, this process may take up to 20 seconds

- If configuring PVC, ensure the VCI values are identical on the switches you are connecting to.
- Verify a PVC Pt-Pt connection is created.

  ```
  /ATM/SHOW >connection
  ```

Troubleshooting Trunking

Problem: **I've created a Trunking service but cannot connect to the ATM network.**

Solution: Use the following solutions:

- Verify that the Trunking service has been created, admin status is enabled, and protocol state is 'active'.

  ```
  /ATM/SHOW/trunk  <trunk id>
  /ATM/CONFIG/ENABLE/trunk <trunk id>
  ```

- If using SVC connections, ensure that the ATM port is configured for SVC mode and ILMI is enabled. By default, the ATM port is set to 'PVC' mode and ILMI is disabled.

  ```
  /ATM/CONFIG/MODIFY> port
  ```

- If using SVC connections, ensure that the ATM port is configured for SVC mode. By default, the ATM port is set to 'PVC' mode.

  ```
  /ATM/CONFIG/MODIFY> port
  ```

- If using SVC connections, ensure that you are using the same UNI signaling version as that of the connected ATM switch.

  ```
  /ATM/CONFIG/MODIFY >port
  ```

- If using SVC connections, verify the following:

  – Port configured as SVC, ILMI enabled, UNI version is correct.

  ```
  /ATM/CONFIG/MODIFY >port
  ```

  – Correct ATM address of destination switch. The last 2 selector bytes needs to be configured as follows:

  Example: `xxx62`
  'xxx' denotes the ATM address defined on the switch. Do a `'vap'` to find out what it is.
  `'6'` is a reserved identifier for Trunking.
  `'2'` identifies the Trunk index configured on the destination switch. Ensure the correct Trunk index is mapped to the switch you are trying to connect to.

  – Verify signaling and ILMI status is 'up'.

  ```
  /ATM/SHOW >port
  ```

- Verify the following using `/ATM/SHOW/connection`:
  - OAM is up.
  - SSCOP, and ILMI is up. *(for SVC only)*
  - A Trunk SVC or PVC connection is created per Trunk instance.
  - ATM port connection and signaling. Operational status, Line state, Signaling status, and ILMI should be ‘up’. (for SVC only)

    ```
    /ATM/CONFIG/MODIFY> port
    ```
- Verify the connection up time is increasing and status is ‘active’ for a specific VCC using `VAC <VCC number>`

Problem: **The Trunk connection is up and active but I cannot ping across the ATM network.**

Solution: Use the following solutions:

- Verify that all IP addresses, subnet masks, gateways are set correctly on the VLANs and any attached devices.
- Verify the ATM port service has been bounded to **all** VLANs. If not, you will need to delete the Port service and re-create it.

  ```
  /PORTSERV/CONFIG >remove <phyport#> <portserv#>
  /PORTSERV/CONFIG/create 34
  vps 34
  ```
- Verify all ATM Trunk ports are in a ‘Forwarding’ state using `vvp`.
  Depending on Spanning Tree, this process may take up to 20 seconds.
- When configuring a PVC connection, ensure the VCI values are identical on the switches you are connecting to. Trunk ids do not need to be the same. However, valid trunk ids range from 0 through 15.

  ```
  /ATM/CONFIG/MODIFY >trunk <trunk id>
  ```

CLI Commands

`/ATM/SHOW >connection`	Displays all active ATM circuits
`/ATM/SHOW >port`	Displays ATM port , Signaling, and ILMI configurations
`/ATM/SHOW >lec , lec <lec#>`	Displays all or a specified LEC status.
`/ATM/SHOW >cip, cip <cip#>`	Displays all or a specified CIP status.
`/ATM/SHOW >ptop, ptop <ptop#>`	Displays all or a specified PTOP status.
`/ATM/SHOW >trunk, trunk <trunk#>`	Displays all or a specified Trunk status.
`/ATM/SHOW/ARP >CIP, LEC`	
`/ATM/CONFIG/`	Commands available for creating/ deleting/modifying and disabling/ enabling ATM services are: • CREATE • DELETE • MODIFY - CIP - LEC - PTOP - TRUNK • DISABLE> - CIP - PTOP - TRUNK
`/ATM/STATS >`	Commands available in displaying ATM statistics. • AAL5 • ATM • CIP • CONNECTION • LEC • PTOP • SIG • TRUNK • UME
`/ATM/SHOW/ARP`	Displays MAC to ATM address mappings • CIP • LEC

Chapter 12
FDDI Concepts

FDDI employes a dual ring topology using two counter-rotating fiber rings: a primary and secondary. Data travels on the primary ring while the secondary backup ring is utilized if the primary ring fails. The data rate is 100 Mbps based on a timed-token access method. The total length of the ring can extend up to 200 kilometers with nodes spaced up to 2 kilometers over multimode fiber.

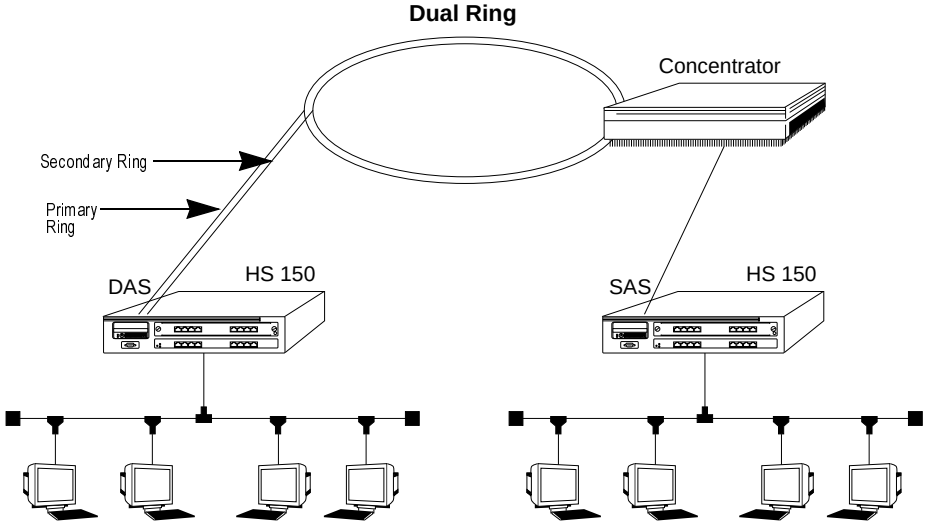


Figure 12-1. HS150 on an FDDI network

In a normal ring operation, an FDDI station captures a free token and transmits completely unless the token holding timer (THT) expires. As the frame traverses the ring, every station examines the frame and checks for errors. When the destination station receives the frame, it copies the frame into its buffer, sets the error, AR, and FC indicators and places the frame back onto the ring. Finally, the frame is returned to the sending station where it is stripped off the ring and the token is released.

Station Management (SMT) unique to FDDI, detects, isolates, and recovers network faults on the ring. The HiSpeed switch participates in the ring recovery process as a function of SMT. Built-in timers are used by all stations to ensure timely transmission of data across the ring. Beacon frames indicate that a logical problem has occurred and the fault domain is identified. Given its error detection and recovery mechanisms, FDDI is considered to be highly reliable and is widely employed as a backbone for local and campus area networks.

HiSpeed FDDI Uplink

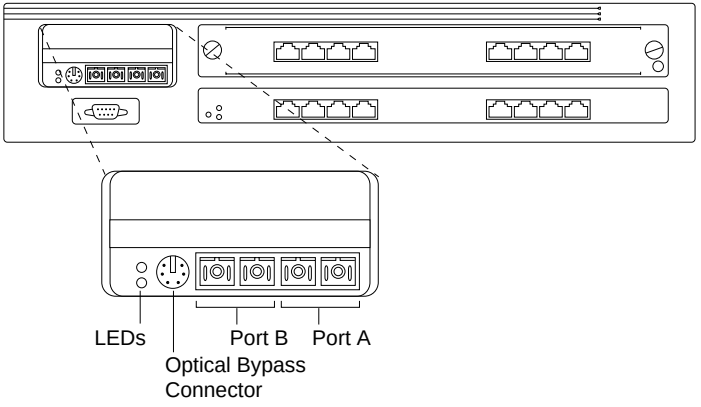


Figure 12-2. FDDI Uplink Module installed in an HS150

The FDDI Uplink module provides fiber optic connectivity between switched 10/100 Ethernet networks and an FDDI backbone network.

Caution: Must be running software version 1.4.4 or later.

Cable Connections

The FDDI Uplink provides two SC connector ports allowing for both a (Single Attached Station) SAS and (Dual Attached Station) DAS configuration.

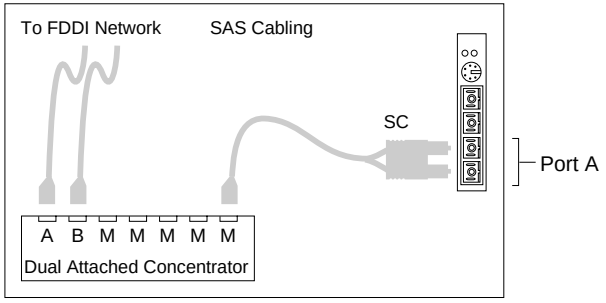


Figure 12-3. SAS cable connections

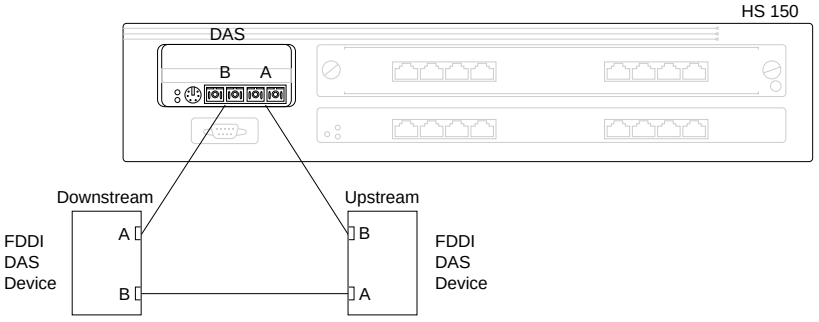


Figure 12-4. DAS cable connections

Observing LEDs

Table 2-1 provides information about what the LEDs mean in various states

Table 12-1. LED States

LED Status		Board Status	Description
Yellow	**Green**		
Off	Off	Fail	Adapter is not functional, or driver is not loaded.
Off	On	Ring Op	Ring operation THRU B (DAS), wrap S for SAS.
On	Off	Cable Error	Adapter not able to connect; possible cable problem.
On	On	Ring Op/ Wrapped	Ring operation: wrap A or B (DAS), unused for SAS.

FDDI Bridge Modes

The HiSpeed switch can operate in any of the following bridging modes:

- ❒ Filtering
- ❒ Forwarding
- ❒ Promiscuous.

The configurations can be set using the following CLI command:

```
/FDDI/CONFIG/BRIDGE/MODE
```

Note: A system reboot is required for the configuration changes to take affect

Filtering Mode

With FDDI Filtering, packets between FDDI-native devices are filtered at the FDDI Uplink, not at the switch's bridging table. This method of filtering reduces the burden on the HiSpeed processor. If the FDDI ring is small and the number of native FDDI devices is limited, FDDI filtering is recommended. Maximum number of entries in the FDDI Filtering table is ***4096***.

Forwarding Mode

With FDDI Forwarding, the MAC addresses of the directly-attached Ethernet devices are placed into the FDDI forwarding table, then only those FDDI packets with destination addresses corresponding in the forwarding table are forwarded to the Ethernet. All other packets are dropped at the FDDI interface, and as a result, reduce the potential load on the HiSpeed processor. If the FDDI ring is very large and the number of directly-attached Ethernet devices is limited, FDDI forwarding should be employed. Maximum number of entries in the FDDI Forwarding table is ***256***.

Promiscuous Mode

With FDDI Promiscuous mode, all packets will be received and forwarded to the FDDI Uplink. This configuration is not recommended as an increased load will be placed on the HiSpeed processor; thereby dramatically reducing the switch's performance.

FDDI Troubleshooting Tips

- ❒ The FDDI Uplink module must be inserted into the lower PCI slot only.
- ❒ A multimode fiber (MMF) cable is required for use with the FDDI uplink module. Each port (A or B) requires a duplex (pair) fiber between two adjacent HS150s. Do not use a simplex (single) fiber to connect two adjacent FDDI ports.
- ❒ FDDI Filtering is the default configuration mode.
- ❒ With Spanning Tree enabled, verify that a virtual port `'34 FDDIBRG'` is active and in a Forwarding state. `'vvp'` or `'vps 34'`
- ❒ Must be running software version 1.4.4 or later.

- ❒ For AppleTalk users, must be running software version 1.3.28 or later.
- ❒ FDDI Port service can only be bounded to VLAN 1. RIP must be ‘active’ to route traffic from one VLAN to another across FDDI.
- ❒ The FDDI driver execution requires five to six seconds longer than the ATM Uplink driver. This is considered normal operation. The initial installation of the FDDI Uplink will delay the login prompt for approximately 30 seconds while the configuration file is updated.

Caution: It is important not to interrupt the boot up sequence during this process by either pressing the front panel Reset switch, or cycling power.

Note: If the HiSpeed Switch is reset by one of these methods during either of the configuration file updates (or even possibly during the driver execution), the FLASH may become corrupted and the switch will subsequently not boot. A FLASH format and Zap of the firmware will be required to recover.

Troubleshooting FDDI:

Problem: **The HiSpeed switch is only forwarding broadcast and multicast traffic but not unicast traffic to an Ethernet device directly attached to the HiSpeed switch.**

Solution: Use the following solutions:

- Verify that physical port 34 is active using `vvp`.
- If the bridge mode is set to Forwarding, verify that the MAC address of the targeted Ethernet device has been learned in the FDDI Forwarding table. This means that either the Ethernet device has to initiate the connection to the switch or reply to an ARP request.

Problem: **I'm having a communication problem with Platelike over FDDI.**

Solution: Use the following solutions:

- Verify that you are running firmware version 1.3.28 or above. In the CLI, enter the `'vsys'` command. If not, upgrade firmware on the switch. Refer to HiSpeed's User Manual for further instructions on how to upgrade the switch.
- Verify that all IP addresses, subnet masks, and gateways are set correctly on the VLANs and any attached devices.

Problem: **Cannot ping another VLAN over FDDI.**

Solution: Use the following solutions:

- Verify that all IP addresses, subnet masks, and gateways are set correctly on the VLANs and any attached devices.
- Verify that all routes are learned using `'vir'`. If not, ensure that RIP is active on all VLANs.

Problem: **The FDDI port does not wrap or unwrap (go back into a ring) under high traffic loads when the cable is removed/attached.**

Solution: This is a known issue and currently there is no fix is available. Resetting the switch will re-initialize the switch back into the ring.

Problem: **FDDI performance is slower from FDDI through Ethernet than from Ethernet through FDDI.**

Solution: There is about 15% difference in the FDDI to Ethernet performance. This is likely the result of employing ARL lookups in software, rather than hardware. There are currently no plans to improve the FDDI through Ethernet performance.

Problem: **I cannot ping to some stations via FDDI.**

Solution: There was a problem in the Hardware Type within the arp packet generated by the HS150. This problem was fixed with 1.4.4. Upgrade your switch the latest version of code. Refer to HiSpeed's User Manual on further instructions on how to upgrade the switch.

Problem: **Traffic through the FDDI port seems to slow and/or hang.**

Solution: There is currently an issue with the FDDI driver and buffer management. Engineering is actively working to resolve the problem. Please contact Hitachi's Internetworking Solution Center for further assistance.

Problem: **The switch appears to hang during the boot up sequence or never reaches the login prompt.**

Solution: Flash memory may have become corrupted. Reformat and Zap flash memory.

CLI Commands

/FDDI/SHOW/MAC>nbraddr	Displays the FDDI MAC Neighbor address table.
/FDDI/SHOW/MAC>status	Checks for the status of the Ring Management state, duplicate address tests, and time values.
/FDDI/SHOW/MAC>stats	Displays the number of tx/rx frames, error frames, copied frames, and thresholds.
/FDDI/SHOW/MAC>counters	Displays the timer expirations, number of tokens, ring operational states.
/FDDI/SHOW/PORT>counters	Reports the number of times the Link Confidence tests passed/failed.
/FDDI/SHOW/PORT>status	Displays the Connect state and PCM state of the switch.
/FDDI/SHOW/PORT>summary	Summary of the SMT Port Configuration.
/FDDI/SHOW/PORT>counters	Reports the number of times the Link Confidence tests passed/failed.
/FDDI/SHOW/SMT>id	Displays the SMT versions and station ID.
/FDDI/SHOW/SMT>status	Displays the SMT station status.
/FDDI/SHOW/SMT>summary	Displays the SMT station configuration table.
/FDDI/CONFIG/BRIDGE >	Used to configure FDDI modes. The following subcommands are available: • ADD • AGE • DELETE • MODE

Index

Symbols

(AR 10-2

(ICM 10-2

(V 11-1

Numbers

010 models 2-4

100 models 2-4

A

Address Resolution Protocol 10-2

alignment errors 9-3

Applications Layer 5-3

Asynchronous Transfer Mode 11-1

ATM 11-1
- CIP diagram 11-4
- CLI commands 11-14
- HiSpeed specifications 11-6
- PTOP diagram 11-5
- troubleshooting tips 11-6
- Trunk diagram 11-5

ATM services 11-2

B

base models 2-2

Boot Prom 3-5

BPDU packets 7-2

bridge
- concepts 7-1
- redundant links 7-1
- root 7-2

bridging modes 12-4

Broadcast and Unknown Server 11-3

BUS 11-3

C

cabling
- 100 Mbps requirements 4-3
- 10BASE-TX ports 4-2
- basic connections 4-1
- FX requirements 4-3
- physical specifications 9-2

changing
- port speed 4-3

changing duplex mode 4-3

Classical IP (CIP) 11-4

CLI commands
- ATM 11-14
- bridge 7-5
- Ethernet 9-5
- FDDI 12-9
- Netwrok layer 10-6

collisions 9-2

Command Line Interface 6-1

configurations
- expansion modules 2-5
- upLink module 2-6

connecting LEC to LECS 11-3

console port
- parameter settings 4-4
- pin assignments 4-4
- using 6-1

CSMA/CD 4-3, 9-1

D

DAS cable connections 12-3

Data Link Layer 5-2

Data loops, eliminating with Spanning Tree 7-1

DB-9 male connecto 4-4

designated bridge 7-3
dribble bits 9-3
dual ring topology 12-1
duplex mode 4-3
duplex mode, setting 4-3
dynamic routes 10-3

E

Ethernet 9-1
  CLI commands 9-5
  tips 9-3
  troubleshooting 9-4
excessive collisions 9-2
expansion modules 2-5
expansion slot 2-3

F

factory default settings 3-5
FCS errors 9-3
FDDI
  bridging modes 12-4
  CLI commands 12-9
  concepts 12-1
  DAS connection 12-3
  filtering 12-5
  Forwarding 12-5
  Promiscuous mode 12-5
  SAS connection 12-3
  Station Management (SMT) 12-2
  troubleshooting tips 12-5
  Uplink module 12-2
features 2-1
fiber ports 4-3
Filtering bridge mode 12-4
Flash 3-5
Forwarding bridge mode 12-4
full-duplex 4-3
Fundamentals of Networking 5-1

G

graphical user interface 6-4

H

half-duplex 4-3
hardware diagnostics 3-1
HiSpeed switch, describe 2-1
HiView
  MeterWare issues 6-7
  SNMPC Issues 6-6
  SNMPTalk Issues 6-10
  tips 6-5
  troubleshooting 6-6
  UNIX version 6-5
  Windows/NT version 6-4
Host Unreachable message 10-4

I

International Standards Organization 5-1
Internet Control Message Protocol 10-2
Internet Protocol 10-1
IP address classes 10-1

L

LAN Emulation 11-2
LAN Emulation Client 11-3
LAN Emulation Configuration Server 11-3
LAN Emulation Server 11-3
LANE 11-2
late collisions 9-2
LEC 11-3
LEC connections to LECS 11-3
LECS 11-3
LED status 3-2
LEDs 3-2
  FX port 3-4
  status lights 12-4
LES 11-3
login 6-3

M

managing, methods 6-1

MDI-X 4-2

memory, standard 3-5

model configurations, table 2-3

models
- HS140/150-010 2-4
- HS140/150-100 2-4

multimode fiber 4-3

N

Network Layer
- CLI commands 10-6
- description 5-3

Network Unreachable message 10-4

Networking, fundamentals 5-1

O

OSI Model 5-1

oversized frames 9-3

P

PCI bus 2-3

Permanent Virtual Circuits 11-2

physical description 4-1

Physical Layer 5-2

physical link 11-1

Point to Point Bridging (PTOP) 11-4

port
- 10/100BASE-TX 4-3
- 100BASE-FX 4-3
- 10BASE-TX 4-2

port configurations 2-2

port speed, changing 4-3

Port Unreachable message 10-4

Presentation Layer 5-3

primary ring 12-1

Promiscuous bridge mode 12-4

protocols, IP-related services 10-2

PVCs 11-2

R

redundant bridge links 7-1

Redundant bridge ports, blocking with Spanning Tree 7-2

Reset button 3-2, 3-3

RIP 10-2

RJ-45
- jacks 4-2

RJ-45 port
- LEDs 3-4

root bridge 7-2

Route Cache Forwarding 10-3

Routing Information Protocol 10-2

S

SAS cable connections 12-3

SC connector 4-3

Session Layer 5-3

Solution Center 1-2

Spanning Tree 7-1
- states 7-3

Spanning Tree Protocol (STP)
- description and overview 7-1

states, Spanning Tree 7-3

static routes 10-3

SVC 11-4

switch, description 4-1

T

TCP 10-2

Tech Support, contacting 1-2

Telnet 6-2

token holding timer (THT) 12-2

Transmission Control Protocol 10-2

Transport Layer 5-3

troubleshooting
basic tips 1-1
CIP 11-8
Ethernet 9-4
FDDI 12-6
HiView 6-6
LANE 11-7
PTOP 11-10
Trunking 11-12
Trunking 11-5

U

UDP 10-2
undersized frames/ runts 9-2
uplink module 2-3
Uplink Module, FDDI 12-2
Uplink modules 2-6
User Datagram Protocol 10-2

V

VCC 11-4
Virtual Channel Connecti 11-1
Virtual Channel Identifi 11-1
Virtual LANs (VLANs)
Spanning Tree Protocol 7-1
Virtual Path Identifie 11-1
VLAN
benefits 8-2
Configuration commands 8-4
configuration subcommands 8-4
tips 8-4
VPI/VCI 11-1